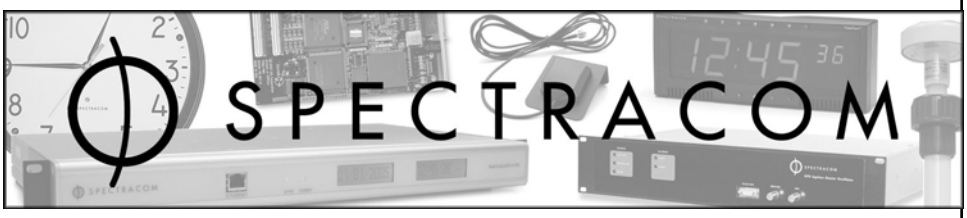
NETCLOCK TIME SERVER
9300 SERIES
INSTRUCTION MANUAL

95 Methodist Hill Drive
Rochester, NY 14623

Phone: US +1.585.321.5800
Fax: US +1.585.321.5219



www.spectracomcorp.com
Part Number 1165-5000-0050
Manual Rev. G
1 July 2009

Copyright © 2009 Spectracom Corporation. The contents of this publication may not be reproduced in any form without the written permission of Spectracom Corporation. Printed in USA.

Specifications subject to change or improvement without notice.

Spectracom, NetClock, Ageless, TimeGuard, TimeBurst, TimeTap, LineTap, MultiTap, VersaTap, and Legally Traceable Time are Spectracom registered trademarks. All other products are identified by trademarks of their respective companies or organizations. All rights reserved.

SPECTRACOM LIMITED WARRANTY

LIMITED WARRANTY

Spectracom warrants each new product manufactured and sold by it to be free from defects in software, material, workmanship, and construction, except for batteries, fuses, or other material normally consumed in operation that may be contained therein AND AS NOTED BELOW, for five years after shipment to the original purchaser (which period is referred to as the "warranty period"). This warranty shall not apply if the product is used contrary to the instructions in its manual or is otherwise subjected to misuse, abnormal operations, accident, lightning or transient surge, repairs or modifications not performed by Spectracom.

The GPS receiver is warranted for one year from date of shipment and subject to the exceptions listed above. The power adaptor, if supplied, is warranted for one year from date of shipment and subject to the exceptions listed above.

THE ANALOG CLOCKS ARE WARRANTED FOR ONE YEAR FROM DATE OF SHIPMENT AND SUBJECT TO THE EXCEPTIONS LISTED ABOVE.

THE TIMECODE READER/GENERATORS ARE WARRANTED FOR ONE YEAR FROM DATE OF SHIPMENT AND SUBJECT TO THE EXCEPTIONS LISTED ABOVE.

The Rubidium oscillator, if supplied, is warranted for two years from date of shipment and subject to the exceptions listed above.

All other items and pieces of equipment not specified above, including the antenna unit, antenna surge suppressor and antenna pre-amplifier are warranted for 5 years, subject to the exceptions listed above.

WARRANTY CLAIMS

Spectracom's obligation under this warranty is limited to in-factory service and repair, at Spectracom's option, of the product or the component thereof, which is found to be defective. If in Spectracom's judgment the defective condition in a Spectracom product is for a cause listed above for which Spectracom is not responsible, Spectracom will make the repairs or replacement of components and charge its then current price, which buyer agrees to pay.

Spectracom shall not have any warranty obligations if the procedure for warranty claims is not followed. Users must notify Spectracom of the claim with full information as to the claimed defect. Spectracom products shall not be returned unless a return authorization number is issued by Spectracom.

Spectracom products must be returned with the description of the claimed defect and identification of the individual to be contacted if additional information is needed. Spectracom products must be returned properly packed with transportation charges prepaid.

Shipping expense: Expenses incurred for shipping Spectracom products to and from Spectracom (including international customs fees) shall be paid for by the customer, with the following exception. For customers located within the United States, any product repaired by Spectracom under a "warranty repair" will be shipped back to the customer at Spectracom's expense unless special/faster delivery is requested by customer.

Spectracom highly recommends that prior to returning equipment for service work, our technical support department be contacted to provide trouble shooting assistance while the equipment is still installed. If equipment is returned without first contacting the support department and "no problems are found" during the repair work, an evaluation fee may be charged.

EXCEPT FOR THE LIMITED WARRANTY STATED ABOVE, SPECTRACOM DISCLAIMS ALL WARRANTIES OF ANY KIND WITH REGARD TO SPECTRACOM PRODUCTS OR OTHER MATERIALS PROVIDED BY SPECTRACOM, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Spectracom shall have no liability or responsibility to the original customer or any other party with respect to any liability, loss, or damage caused directly or indirectly by any Spectracom product, material, or software sold or provided by Spectracom, replacement parts or units, or services provided, including but not limited to any interruption of service, excess charges resulting from malfunctions of hardware or software, loss of business or anticipatory profits resulting from the use or operation of the Spectracom product or software, whatsoever or howsoever caused. In no event shall Spectracom be liable for any direct, indirect, special or consequential damages whether the claims are grounded in contract, tort (including negligence), or strict liability.

EXTENDED WARRANTY COVERAGE

Extended warranties can be purchased for additional periods beyond the standard five-year warranty. Contact Spectracom no later than the last year of the standard five-year warranty for extended coverage.

SPECTRACOM 95 Methodist Hill Drive Rochester, NY 14623

+1.585.321.5800 FAX: +1.585.321.5218 www.spectracomcorp.com sales@spectracomcorp.com

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

.

Table of Contents

1 THE 9300 SERIES NETCLOCK 1-1
1.1 Introduction 1-1
1.2 Inputs and Outputs: What Can the NetClock Do for You? 1-1
1.2.1 Front Panel 1-2
1.2.2 Front Panel LED Indicators 1-2
1.2.3 Front Panel LED Status Indications 1-2
1.3 Rear Panel 1-3
1.4 Warranty Information and Customer Support 1-4
1.5 Specifications 1-5
1.5.1 Receiver 1-5
1.5.2 RS-232 Serial Setup Interface Port 1-5
1.5.3 10/100 Ethernet Port 1-5
1.5.4 Protocols Supported 1-5
1.5.5 RS-232 Communication Port 1-6
1.5.6 RS-485 Output 1-6
1.5.7 Relay Outputs 1-6
1.5.8 IRIG Output 1-7
1.5.9 1PPS Output 1-7
1.5.10 1PPS Input Specifications 1-8
1.5.11 Frequency Output 1-8
1.5.12 Input Power 1-8
1.5.13 Mechanical and Environmental 1-8
2 INSTALLATION 2-1
2.1 Inspection 2-1
2.1.1 Inventory 2-1
2.2 Summary 2-2
2.3 Required Tools and Cables 2-5
2.4 Power and Ground Connection 2-5
2.5 Rack Mounting 2-6
2.6 GPS Antenna Installation 2-6
2.6.1 Antenna Cable for Outdoor Antenna 2-6
2.6.2 Cable Lengths 2-6
2.6.3 Model 8224 GPS Splitter 2-8
2.6.4 Model 8226 Impulse Suppressor 2-8
2.6.5 Model 8227 GPS Inline Amplifier 2-9
2.7 Ethernet Network Cabling 2-10
2.7.1 Optional CNC3000 Cable Kit 2-10
2.8 Remote Port and Serial Comm Port Output Pin-outs and Wiring 2-11
2.8.1 Serial Comm Ports 2-11
2.8.2 RS-485 Remote Port 2-12
2.8.3 Remote Output Usage 2-13
2.8.4 RS-485 Guidelines and Cable Selection 2-13
2.8.5 Connection Method 2-14
2.8.6 Termination 2-18
3 PRODUCT CONFIGURATION 3-1
3.1 Network Configuration with DHCP 3-2
3.2 Initial Network Configuration 3-5
3.2.1 Using HyperTerminal to Connect to the NetClock 3-5

3.2.2 Initial Network Setup 3-9
3.2.3 Default and Recommended Configurations 3-12
3.3 Issuing the HALT Command before Removing Power 3-13
3.3.1 Issuing the HALT Command through the Web UI 3-13
3.3.2 Issuing the HALT Command through the CLI 3-15
3.3.3 Issuing the HALT Command through SNMP 3-16
3.4 Product Configuration using the WEB UI 3-19
3.4.1 Configuring NTP 3-19
3.4.2 NTP Support 3-28
3.4.3 Configuring the Interface 3-29
3.4.4 Sysplex Timing 3-44
3.4.5 Configuring the System: SNMP 3-45
3.4.6 Configuring Alarms 3-48
3.4.7 Configuring GPS 3-49
3.4.8 Configuring System Time and Local Clocks 3-51
3.4.9 Setting the System Mode 3-58
3.4.10 Activating System Options and Rolling Back Updates 3-59
3.4.11 Rebooting the System 3-61
3.4.12 Configuring System Holdover 3-62
3.4.13 Configuring 1PPS Input 3-64
3.4.14 Serial Time Code Setup 3-65
3.4.15 Configuring System Logs 3-67
3.4.16 Configuring and Testing Relays 3-69
3.4.17 Configuring Network Security 3-78
3.4.18 If You Cannot Access a Secure NetClock 3-90
3.4.19 Configuring User Accounts 3-91
3.4.20 Configuring SNMP v1, v2, and v3 3-93
3.4.21 Configuring LDAP and RADIUS 3-97
3.4.22 Configuring IPSec 3-101
3.4.23 Logs and Status Reporting 3-112
4 DAY-TO-DAY OPERATION 4-1
4.1.1 Event and Alarm Relay Outputs 4-1
4.2 Leap Second occurrence 4-2
4.2.1 Reasons for a Leap Second Correction 4-2
4.2.2 Leap Second Alert Notification 4-2
4.2.3 Sequence of a Leap Second Correction Being Applied 4-3
5 SERIAL DATA FORMATS 5-1
5.1 Format 0 5-1
5.2 Format 1 5-2
5.3 Format 2 5-4
5.4 Format 3 5-6
5.5 Format 4 5-7
5.6 Format 7 5-8
5.7 Format 8 5-10
5.8 Format 90 5-11
6 SERIAL SETUP INTERFACE COMMANDS 6-1
6.1 time 6-1
6.2 reboot 6-1
6.3 log 6-2
6.4 option 6-2
6.5 ltc 6-2

6.6 net ... 6-3
6.7 sys ... 6-3
6.8 mdo ... 6-3
6.9 ser ... 6-4
6.10 rem ... 6-4
6.11 irig ... 6-4
6.12 frq ... 6-5
6.13 stc ... 6-5
7 OPTIONS ... 7-1
7.1 Option 03: Modem ... 7-1
7.1.1 Option 03 Basics ... 7-1
7.1.2 Modem Installation ... 7-2
7.1.3 Modem Configuration ... 7-2
7.1.4 ACTS Server Mode ... 7-5
7.1.5 Modem Dial-Out Setup ... 7-9
7.1.6 Modem Dialout ... 7-10
7.1.7 Modem Testing ... 7-14
7.1.8 Verify Modem Operation ... 7-16
7.2 Option 04: Rubidium Oscillator ... 7-19
7.2.1 Comparison of the Rubidium oscillator to the OCXO and standard TCXO oscillators: ... 7-19
7.3 Option 05: OCXO Oscillator ... 7-20
7.3.1 Comparison of the OCXO to the Rubidium and Standard TCXO oscillators: ... 7-20
7.4 Option 06: IRIG Input ... 7-21
7.4.1 IRIG Input Specifications ... 7-21
7.4.2 IRIG Input Setup ... 7-22
7.5 Option 07: SAASM ... 7-23
7.5.1 Satellite Mode ... 7-24
7.5.2 Satellite Status ... 7-24
7.5.3 Zeroize ... 7-24
7.5.4 Security — SAASM ... 7-25
7.6 Option 10: Low Phase Noise Rubidium 10 MHz and Differential IRIG Output ... 7-26
7.6.1 10 MHz Output (FREQ OUT) Specifications ... 7-26
7.6.2 IRIG-B Output (Remote Port 2) Specifications ... 7-26
7.6.3 DC Input Power ... 7-26
7.6.4 Rear Panel Connectors ... 7-26
7.7 Option 11: Modified IRIG Output ... 7-27
7.7.1 IRIG-B Output Specifications ... 7-27
7.7.2 IRIG-E Output Specifications ... 7-27
7.7.3 ASCII Time Code Output (Format 09) ... 7-27
7.7.4 DC Input Power ... 7-27
7.7.5 Serial Port 2 (Format 09) Configuration ... 7-28
7.7.6 Rear Panel Connectors ... 7-28
8 LICENSE NOTICES ... 8-1

List of Figures

Figure 1-1: Front Panel Display ... 1-2
Figure 1-2: NetClock Rear Panel ... 1-3
Figure 2-1: Cabling without Inline Amplifier ... 2-7
Figure 2-2: Cabling with Inline Amplifier ... 2-8
Figure 2-3: Model 8226 Impulse Suppressor ... 2-9

Figure 2-4: Model 8227 Inline Amplifier 2-9
Figure 2-5: Serial Port Pin Configuration 2-11
Figure 2-6: Remote Outputs 2-12
Figure 2-7: RS-485 Output 2-13
Figure 2-8: One-Way Bus Installation 2-14
Figure 2-9: Split Bus Configuration 2-15
Figure 2-10: Wire Strain Relief 2-16
Figure 2-11: TimeView RS-485 Interface 2-16
Figure 2-12: Model 8179T TimeTap RS-485 Interface 2-17
Figure 2-13: Model 9288 RS-485 Interface 2-17
Figure 2-14: TimeBurst RS-485 Interface 2-18
Figure 3-1: Entering to the Configuration in the Web UI 3-1
Figure 3-2: Web Browser User Interface (Web UI) 3-2
Figure 3-3: Security – Network Screen (1 of 2) 3-3
Figure 3-4: Security – Network Screen (2 of 2) 3-4
Figure 3-5: Establishing a New Terminal Connection 3-5
Figure 3-6: Connecting to the Computer's Serial Port 3-6
Figure 3-7: Configuring the Serial Port Connection Properties 3-6
Figure 3-8: Spectracom NetClock Command Line Interface (CLI) 3-7
Figure 3-9: Available CLI Commands 3-7
Figure 3-10: Serial Port Pin Configuration 3-8
Figure 3-11: Net Commands 3-9
Figure 3-12: Prompt for Initial Configuration Values in the CLI 3-9
Figure 3-13: Initial Configuration using the CLI 3-10
Figure 3-14: Successful Completion of Network Configuration 3-11
Figure 3-15: System Reboot/Halt Screen (1 of 3) 3-13
Figure 3-16: System Reboot/Halt Screen (2 of 3) 3-14
Figure 3-17: System Reboot/Halt Screen (3 of 3) 3-14
Figure 3-18: Command Line Interface (CLI) 3-15
Figure 3-19: Halting the System from the CLI 3-15
Figure 3-20: Rebooting the System from the CLI 3-16
Figure 3-21: Reboot MIB Location Options (SNMP) 3-16
Figure 3-22: Rebooting the Unit through SNMP 3-17
Figure 3-23: Halting the Unit through SNMP 3-18
Figure 3-24: Successful Halt 3-18
Figure 3-25: Web UI Primary Menu 3-19
Figure 3-26: Web UI NTP Menu 3-19
Figure 3-27: NTP General Screen 3-20
Figure 3-28: NTP References Screen (1 of 2) 3-23
Figure 3-29: NTP References Screen (2 of 2) 3-24
Figure 3-30: NTP Symmetrical Keys Screen 3-25
Figure 3-31: NTP Autokey Screen 3-26
Figure 3-32: Statistics FTP Screen 3-27
Figure 3-33: NTP Status Screen 3-28
Figure 3-34: Interface Menu 3-29
Figure 3-35: Interface Serial Port 1 Screen 3-30
Figure 3-36: Interface Remote Port 2 Screen 3-31
Figure 3-37: Interface IRIG Screen 3-32
Figure 3-38: IRIG Output Level 3-34
Figure 3-39: IRIG B Time Code description 3-35
Figure 3-40: IRIG E Time Code Description 3-39

Figure 3-41: Interface Front Panel Display Screen 3-41
Figure 3-42: Interface Frequency Output Screen 3-42
Figure 3-43: Interface Set to Defaults Screen 3-43
Figure 3-44: Configuring Serial Port 1 for Sysplex Timing 3-44
Figure 3-45: System Menu 3-45
Figure 3-46: System SNMP Screen 3-46
Figure 3-47: Spectracom's MIB 3-47
Figure 3-48: System Alarm Screen 3-48
Figure 3-49: System GPS Screen 3-50
Figure 3-50: System Time Screen 3-51
Figure 3-51: Local System Clock Screen (1 of 3) 3-52
Figure 3-52: Local System Clock Screen (2 of 3) 3-53
Figure 3-53: Local System Clock Screen (3 of 3) 3-54
Figure 3-54: System Mode Screen 3-59
Figure 3-55: System Update Screen 3-60
Figure 3-56: System Reboot Screen 3-61
Figure 3-57: System Holdover Screen 3-63
Figure 3-58: System Status Screen (1PPS Input Indicated) 3-65
Figure 3-59: Serial Time Code Setup Screen 3-66
Figure 3-60: System Log Configuration Screen (1 of 2) 3-67
Figure 3-61: System Log Configuration Screen (2 of 2) 3-68
Figure 3-62: Relay Menu 3-69
Figure 3-63: Relay Output Screen 3-70
Figure 3-64: Event Timer Relay Screen 3-71
Figure 3-65: Edit/View Event Timers 3-72
Figure 3-66: Relay Current Event Scheduler Screen 3-74
Figure 3-67: Relay Reset ALL Event Timers Screen 3-75
Figure 3-68: Set Event Clock Screen 3-76
Figure 3-69: Test Relays Screen 3-77
Figure 3-70: Security Menu 3-78
Figure 3-71: Security Network Screen (1 of 2) 3-79
Figure 3-72: Security Network Screen (2 of 2) 3-80
Figure 3-73: Security SSH Screen (1 of 2) 3-81
Figure 3-74: Security SSH Screen (2 of 2) 3-82
Figure 3-75: Security HTTPS Screen (1 of 2) 3-87
Figure 3-76: Security HTTPS Screen (2 of 2) 3-88
Figure 3-77: Security User Account Screen 3-91
Figure 3-78: Security User Account Screen (Assigning Privileges) 3-92
Figure 3-79: SNMP Security Screen (1 of 3) 3-93
Figure 3-80: SNMP Security Screen (2 of 3) 3-94
Figure 3-81: SNMP Security Screen (3 of 3) 3-95
Figure 3-82: Security LDAP General Screen 3-96
Figure 3-83: Security LDAP Client Configuration Screen (1 of 2) 3-97
Figure 3-84: Security LDAP Client Configuration Screen (2 of 2) 3-98
Figure 3-85: Security RADIUS General Screen 3-99
Figure 3-86: Security RADIUS Client Configuration Screen 3-100
Figure 3-87: IPSEC IKE SA Configuration Screen (1 of 2) 3-102
Figure 3-88: IPSEC IKE SA Configuration Screen (2 of 2) 3-103
Figure 3-89: IPSec General Screen 3-106
Figure 3-90: IPSec Manual SA Configuration (1 of 2) 3-108
Figure 3-91: IPSec Manual SA Configuration (2 of 2) 3-109

Figure 3-92: IPSec General Screen 3-110
Figure 3-93: Status and Log Menu 3-112
Figure 3-94: Alarm Log Screen 3-113
Figure 3-95: Authorization Log Screen 3-114
Figure 3-96: Event Log Screen 3-115
Figure 3-97: GPS Qualification Log Screen 3-116
Figure 3-98: Journal Log Screen 3-117
Figure 3-99: NTP Log Screen 3-118
Figure 3-100: IKE Log Screen 3-119
Figure 3-101: Operational Log Screen 3-120
Figure 3-102: Oscillator Log Screen 3-121
Figure 3-103: System Log Screen 3-122
Figure 3-104: Update Log Screen 3-123
Figure 3-105: GPS Signal Status Screen 3-124
Figure 3-106: NTP Status Screen 3-126
Figure 3-107: System Status Screen (1 of 2) 3-127
Figure 3-108: System Status Screen (2 of 2) 3-128
Figure 4-1: Event and Alarm Relay Contacts 4-1
Figure 7-1: Modem Switches 7-2
Figure 7-2: System Modem Configuration Screen, Console Mode 7-3
Figure 7-3: System Modem Configuration Screen, Client Mode 7-4
Figure 7-4: ACTS Server Mode Selected 7-5
Figure 7-5: ACTS Server Greeting 7-7
Figure 7-6: ACTS Server Statistics 7-8
Figure 7-7: ACTS Server Log 7-9
Figure 7-8: System Modem Dial Out Screen (1 of 2) 7-11
Figure 7-9: System Modem Dial Out Screen (2 of 2) 7-12
Figure 7-10: System Modem Calibrate Screen 7-13
Figure 7-11: Modem Test Screen 7-15
Figure 7-12: Modem Dialout Log Screen 7-17
Figure 7-13: IRIG Input Screen 7-22
Figure 7-14: GPS Signal Status 7-23
Figure 7-15: Zeroize Screen 7-25
Figure 7-16: Serial Port Configuration 7-28

Underwriters Laboratory (UL) has not tested the performance or reliability of the Global Positioning System (GPS) hardware, operating software, or other aspects of this product. UL has only tested for fire, shock, or casualties as outlined in UL's Standard(s) for Safety for Information Technology Equipment, UL60950-1. UL Certification does not cover the performance or reliability of the GPS hardware and GPS operating software.

UL MAKES NO REPRESENTATIONS, WARRANTIES, OR CERTIFICATIONS WHATSOEVER REGARDING THE PERFORMANCE OR RELIABILITY OF ANY GPS RELATED FUNCTIONS OF THIS PRODUCT.

1 The 9300 Series NetClock

Spectracom Corporation is a leading manufacturer of precise time-keeping devices used to synchronize critical operations. Our products provide accurate, reliable, Legally Traceable Time™ across your networks. The Spectracom 9300 series NetClock™ is a direct response to customer needs for affordable time synchronization equipment that includes a variety of necessary and widely used security, authentication, and networking features.

1.1 Introduction

The 9300 Series NetClock time server provides disciplined timing using Network Time Protocol (NTP). The NetClock meets or exceeds the National Emergency Numbers Association (NENA) master clock standard and is ideally suited for delivering world-wide, split-second timing to mission critical systems. The 9300 series offers enhanced reliability features, including oven-stabilized crystal oscillator (OCXO) and Rubidium oscillator backups to maintain the NetClock's time standard if the time reference is lost. An optional dial-out modem provides additional back-u and can function as the primary reference if desired. The 9300 series chassis is shock- and vibration-resistant.

The 9300 series' enhanced security features, which can be enabled and disabled by the user, include IPSec, Secure Shell (SSH), Secure Sockets Layer (SSL), Secure Copy Protocol (SCP), Secure File Transfer Protocol (SFTP), and SNMP v1, v2, and v3 with host access restriction. The NetClock supports IPv4, IPv6, and centralized user authentication (LDAP/Active Directory, RADIUS). NTP capabilities include peering, Stratum 2, and Autokey.

The NetClock can be configured and its reports accessed through a Web User Interface (Web UI). A Command Line Interface (CLI) is also provided for initial product configuration through the serial setup port. Once configured, the NetClock can be accessed, under appropriate security policies, anywhere within a network. The product features browser-based remote diagnostics and control as well as Flash memory for remote software upgrades. A 10/100 Mbps Ethernet LAN port provides support for Network Time Protocol (NTP) over a variety of platforms, including Windows 2003, 2000, and XP, Cisco, UNIX, Linux, and more. Remote control and monitoring can also be performed through SNMP and Telnet.

NOTE: All features described are not available on all NetClock variants.

1.2 Inputs and Outputs: What Can the NetClock Do for You?

Spectracom NetClocks provide multiple outputs for use in networked devices and other pieces of technology. A 1 Pulse Per Second (1PPS) output acts as a precise metronome, counting off seconds of UTC time. A 10 MHz frequency reference provides a precise, disciplined signal for control systems and clocks (as the inverse of time is frequency). IRIG output, used in many military and some public safety and data centers, provides a time code for time-stamping of data, as do the NetClock's serial time code outputs.

The NetClock's outputs are driven by its inputs – specifically, IRIG, serial time code, and (most significantly) Global Positioning System (GPS) technology. GPS-equipped NetClocks track up to twelve satellites simultaneously and synchronize to the satellite's atomic clocks. This enables

NetClock-equipped computer networks to synchronize all elements of network hardware and software (including system logs) over LANs or WANs – anywhere on the planet.

1.2.1 Front Panel

The front panel of the NetClock (Figure 1-1) consists of two separate, illuminated status LEDs and two LCD displays (depending on the model). The LCDs (when installed) are configurable using the Web Browser User Interface (Web UI). Options include time, date, day of year, software versions, network information, fonts, and date formats.

The status LEDs, "Sync" and "Power," indicate whether the NetClock is synchronized and whether power is applied to the unit. The Power LED will not light if power is not applied. It will indicate green if power is applied. The Sync LED has multiple states (Table 1-1).

Figure 1-1: Front Panel Display

1.2.2 Front Panel LED Indicators

Power: Green, always on.

Sync: Tri-color LED indicates the time data accuracy and equipment fault.

LAN: Green: Good Link indicator.

Yellow: Network activity.

1.2.3 Front Panel LED Status Indications

At power up, a quick LED test is run. The unit displays a ***Red*** – ***Green – Orange*** sequence.

LABEL	COLOR	ACTIVITY	DESCRIPTION
POWER	Green	On Off	Power is supplied to the NetClock. Power is disconnected.
SYNC	Multiple States	Off	No fault but not synchronized to GPS. Holdover spec has not been met.
		Green On	Synchronized to GPS. Time is valid and within the Locked to GPS accuracy specs.
		Blinking Green	Holdover mode. Not synchronized to GPS but time is still within Holdover accuracy specs. Also indicates the unit is synchronized with the optional dial-out modem (Option 03).
		Yellow On	No longer synchronized to GPS but no unit fault. Time accuracy may not be meeting holdover specs.
		Blinking Yellow	Unit is in power-up initialization mode. The unit is in this mode for the brief period between power on and when it is operationally ready to receive satellite data.
		Flashing Red	GPS antenna fault. This flash may occur over any of the other color conditions at runtime.
		Red On	Unit fault. Time may not be valid. Overrides all other indicators.
		Blinking Red	If the unit fails Power On Self Test (POST) then the indicator will blink in a sequence indicating the failure code (consult factory)

Blink is defined as ½ second on, ½ second off
Flash is defined as $^{1}/_{20}$ second on, $^{19}/_{20}$ second off

Table 1-1: Status Indicators, Front Panel

1.3 Rear Panel

The rear panel (Figure 1-2) provides several different outputs that are available for interfacing the NetClock to various systems, as well as a means of initially configuring the unit's network settings. The rear panel also has a power jack for the power input, a connection for the GPS antenna, and relay contacts for alarm monitoring and event alerts.

Figure 1-2: NetClock Rear Panel

FREQ OUT is a BNC output providing a 10MHz sinewave output.

1PPS OUT is a BNC output providing a once-per-second squarewave output.

IRIG OUT is a BNC output providing an IRIG signal for synchronizing certain voice recorders.

1PPS IN is a BNC female input used to provide an external 1PPS reference.

Serial Comm 1 and **Serial Comm 2** are "DB9 female" connectors that provide RS-232 data output to devices that can accept an RS-232 input for synchronization.

The two RS-485 connectors (**RS-485 PORT 1 and PORT 2**) provide an RS-485 data output for synchronizing devices that accept an RS-485 input, such as wall display clocks and add-on Ethernet Time Servers.

The **SERIAL SETUP INTERFACE** provides network and output port configuration capability.

The **ETHERNET** connector provides an interface to the network for NTP synchronization and to obtain access to the Web UI. It has two small indicator lamps, Good Link (green LED) and Activity (orange LED). The Good Link light indicates a connection to the network is present. The activity light will blink when network traffic is detected.

Ethernet	Yellow	On Off	LAN Activity detected. No LAN traffic detected.
Ethernet	Green	On Off	LAN Link established 10 or 100 Mb/s. No link established.

Blink is defined as ½ second on, ½ second off
Flash is defined as $^{1}/_{20}$ second on, $^{19}/_{20}$ second off

Table 1-2: Status Indicators, Rear Panel

TIMER/ALARM RELAYS 1, 2, and **3** are configurable for remote alerts and monitoring.

The **GPS ANTENNA** connection is an "N" type connector for the GPS input from the antenna.

The **POWER** connector is the input for the DC power.

The **CHASSIS GROUND** connector provides a means of grounding the unit.

1.4 Warranty Information and Customer Support

Warranty information is found on the leading pages of this manual.

Spectracom constantly strives to improve its products. We greatly appreciate any and all customer feedback.

Technical support is available by telephone at **US +1.585.321.5800**. Please direct any comments or questions regarding application, operation, or service to Spectracom's Customer Service Department. Customer Service is available Monday through Friday from 8:00 a.m. to 5:00 p.m. EST, excluding holidays.

Product support is also available by e-mail. Questions regarding equipment, operation, and applications may be e-mailed to Spectracom Sales Support at:

sales@spectracomcorp.com

For repairs and technical support, questions may be e-mailed to Spectracom Technicians at:

techsupport@spectracomcorp.com

Visit Spectracom's web page for product information, application notes, and upgrade notices as they become available:

http://www.spectracomcorp.com/

Please contact Customer Service before returning any equipment Spectracom. Customer Service must provide you with a Return Material Authorization Number (RMA#) prior to shipment. When contacting Customer Service, please be prepared to provide your equipment serial number(s) and a description of the failure symptoms or issues you would like resolved. Freight to Spectracom is to be prepaid by the customer.

Once you have obtained the RMA number, ship your equipment to the following address:

Spectracom Corporation
Repair Department, RMA# xxxxx
95 Methodist Hill Drive
Rochester, NY 14623

1.5 Specifications

NOTE: The specifications listed herein are based on "standard" operation, with the unit synchronized to GPS and with the GPS receiver in position hold (or the equivalent for non-GPS units).

1.5.1 Receiver

Received standard:	L1 C/A Code transmitted at 1575.42 MHz.
Satellites tracked:	Up to twelve simultaneously.
Acquisition time:	Typically <4 minutes from a cold start.
Antenna requirements:	Active antenna module, +5V, powered by the NetClock, 16 dB gain minimum.
Antenna connector:	Type N, female.

1.5.2 RS-232 Serial Setup Interface Port

Function:	Accepts commands to locally configure the IP network parameters for initial connectivity. Also used as the interface to the dial-out modem (Option 03).
Connector:	DB9 female, pin assignments conform to EIA/TIA-574 standard, data communication equipment.
Character structure:	ASCII, 9600 baud, 1 start, 8 data, 1 stop, no parity.

1.5.3 10/100 Ethernet Port

Function:	10/100 BaseT auto sensing LAN connection for NTP / SNTP and remote monitoring, diagnostics, configuration and upgrade.

1.5.4 Protocols Supported

NTP:	NTP v4.2.0. Provides MD5 and Autokey. Stratum 1 or higher. (RFC 1305, 4330)
Loading:	~4,000 requests per second, typical.
Clients supported:	The number of users supported depends on the class of network and the subnet mask for the network.
	A gateway greatly increases the number of users.
HTTP, HTTPS Servers:	For browser-based configuration and monitoring using Internet Explorer 5 or Netscape 6 per RFC 1945 and 2068.
FTP:	For remote upload of system logs and RFC 959.
Logging:	Syslog
SNMP:	Supports v1, v2c, and v3
Telnet:	For limited remote configuration per RFC 854.

Security Features:	Up to 32-character password, Telnet Disable, FTP Disable, Secure SNMP, SNMP Disable, HTTPS, HTTP Disable, SCP, SSH, SFTP.
Authentication:	LDAP v2 and v3, RADIUS, MD5 Passwords, NTP Autokey Protocol.
Connector:	RJ-45, Network IEEE 802.3.

1.5.5 RS-232 Communication Port

Signal:	Selected time Data Format in RS-232 levels when interrogated by the connected device. This port may also be configured to provide a continuous once-per-second output.
Connector:	DB9 female, pin assignments conform to EIA/TIA-574 standard, data communication equipment (DCE). No flow control.
Character structure:	ASCII, 1 start, 8 data, 1 stop, and no parity.
Accuracy:	Data stream on time marker within ± 100 microseconds of UTC on Sync in Data Formats 0, 1, 3 and 8. Data Formats 2, 4 and 7 within ±1 millisecond of UTC.
Configuration:	Baud rate and output Data Formats are selected using the web browser user interface. Bit rate selections are 1200, 2400, 4800 and 9600 baud. There are eight Data Format selections available.

1.5.6 RS-485 Output

Signal:	Selected time Data Format in RS-485 levels, output once-per-second.
Connector:	Removable 3-position terminal block (supplied).
Character structure:	ASCII, 1 start, 8 data, 1 stop, and no parity.
Accuracy:	Data stream on time marker within ± 100 microseconds of UTC on Sync in Data Formats 0, 1, 3 and 8. Data Formats 2, 4 and 7 within ±1 millisecond of UTC.
Configuration:	Baud rate and output Data Formats are selected using the web browser user interface. Bit rate selections are 1200, 2400, 4800, and 9600 baud. There are eight Data Format selections available.

1.5.7 Relay Outputs

Three separate outputs provided for either Programmable Event Timer Output or Major/Minor Alarm indication.

Relay contacts:	NO, NC, and Common.
Contact rating:	30 VDC, 2 amps.
Connector:	10-position 3.81 mm terminal block (mate supplied).

Programmable Timer Output:

128 On/Off events available. Timer events that are hourly, daily or weekly only count as a single event so many events can be programmed.

Major/Minor Alarms: Relay contacts allow remote monitoring of operational status. A power failure, CPU failure loss of time sync, etc cause the alarm relay to de-energize. The alarm relay returns to normal operation (energized) when the fault condition is corrected.

1.5.8 IRIG Output

Signal: Selectable IRIG B or IRIG E, amplitude modulated sine wave (AM) or pulse-width-coded (TTL/DCLS).

AM Carrier: IRIG B-1000 Hz.
IRIG E-100 Hz or 1000 Hz.

AM Signal Level: Adjustable from 0 to 10 Vp-p mark amplitude into loads of 600 ohms. Factory set to 2.0 V p-p into 600 ohms. Output should be terminated with 600 ohms.

Accuracy: IRIG-B, IRIG-E 1000 Hz AM: ±20 microseconds of UTC. IRIG-E 100 Hz AM: 200 microseconds of UTC. IRIG-B, IRIG-E TTL/DCLS: ±2 microseconds of UTC.

Connector: BNC female.

Configuration: IRIG Formats B or E in AM or TTL/DCLS levels. Time data is configurable with Time Zone Offsets and DST rules. Signature Control may also be placed on the output signal. This feature removes the modulation code from the IRIG output whenever the selected alarm condition is present. The output is restored when the fault is corrected.

IRIG Code Format	Description of code
B000	IRIG B, TTL, BCD,CF and SBS
B120	IRIG B, AM, 1 kHz , BCD,CF and SBS
E000	IRIG E TTL, BCD,CF and SBS
E110	IRIG E AM, 100 Hz, BCD,CF and SBS
E120	IRIG E AM, 1 kHz, BCD,CF and SBS

1.5.9 1PPS Output

Signal: One pulse-per-second square wave derived from the GPS receiver.

Signal Level: TTL compatible into high impedance loads, 1.5 V base-to-peak into 50 ohms.

Pulse Width: 200 milliseconds.

Accuracy: Positive edge within ± 50 nanoseconds of UTC when locked to GPS.

Connector: BNC female.

1.5.10 1PPS Input Specifications

Signal:	One pulse-per-second square wave.
Signal Level:	TTL compatible (High trigger is 2.1 V, low is 0.9 V), High Z (> 10k ohms), Active rising edge.
Connector:	BNC female.

1.5.11 Frequency Output

Signal:	10 MHz sinewave.
Signal Level:	700 mVrms into 50 ohms.
Harmonics:	-30 dBc minimum.
Spurious:	-35 dBc minimum.
Oscillator Accuracy:	**TCXO** (Standard): $1x10^{-10}$ typical 24-hour average locked to GPS.
	OCXO (Option 05): $1x10^{-11}$ typical 24-hour average locked to GPS, $2x10^{-9}$ per week typical aging unlocked.
	Rubidium (Option 04): $1x10^{-12}$ typical 24-hour average locked to GPS; $1x10^{-11}$ per month typical aging unlocked.
Connector:	BNC female
Signature Control:	This configurable feature removes the output signal whenever a major alarm condition or loss of time synchronization condition is present. The output is restored when the fault condition is corrected.

1.5.12 Input Power

Power source:	90 to 240 VAC, 47 to 63 Hz through an IEC 320 universal connector.
DC input:	9.5 to 30 VDC, 18 watts, through a CE/UL/CSA-approved power adapter (supplied).
	NOTE: Rubidium (Option 04) uses a 24 VDC nominal (+18 – +32 VDC) @ 2.5 amps power supply.
Connector:	Terminal Block, 3 pin pluggable with screw locks, 5.08 mm.
Polarity:	Negative shell, positive center.

1.5.13 Mechanical and Environmental

Dimensions:	Designed for EIA 19” rack mount
	16.75” W x 1.72” H [1U] x 14.00” D actual
	(425 mm W x 44 mm H x 356 mm D) actual
Weight:	6.5 lbs. (2.95 kg) with Rubidium option; 6.0 lbs (2.72 kg) without
Temperature:	32° to 122°F (0° to 50°C) operating range
	-40° to 185°F (-40° to 85°C) storage range
Humidity:	10% - 95% relative humidity, non-condensing

2 Installation

2.1 Inspection

On receipt, carefully examine the carton and its contents.

CAUTION: *Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling Spectracom equipment.*

Verify that all material ordered has been received by checking the carton contents against the packing list. If there is a discrepancy, please contact Spectracom Customer Service at US +1.585.321.5800. If there is damage to the carton resulting in damage to the unit, contact the carrier immediately. Retain the carton and packing materials in the event the carrier wishes to witness the shipping damage. Failing to report shipping damaging immediately may forfeit any claim against the carrier. In addition, notify Spectracom Corporation of shipping damage or shortages in order to obtain a replacement or repair services.

NOTE: If equipment is returned to Spectracom, it must be shipped in its original packing material. Save all packaging material for this purpose.

2.1.1 Inventory

Your Spectracom time server package ships with the following components:

- ☐ Unit
- ☐ User manual
- ☐ CE/UL-approved power supply for international use
- ☐ Standard DB9F to DB9M RS-232 cable pinned as straight thru (used for initial configuration)
- ☐ AC power cord
- ☐ Rack-mount kit
- ☐ Rubber footpads for desktop installation
- ☐ 3-pin terminal block connector for RS-485 connections
- ☐ 10-pin terminal block connector
- ☐ Jeweler's type screwdriver (for tightening the screws on the terminal blocks)
- ☐ Terminating Resistors, 120Ω

Spectracom models that have the modem dial-out feature (Option 03) ship with a serial modem kit.

2.2 Summary

This section provides an overview summary of the installation process. The installation of the NetClock consists of the following steps. Refer to the table of contents in this manual for specific section references detailing how these summarized steps are accomplished.

WARNING:

This equipment has a connection between the earthed conductor of the DC supply circuit and the earthing conductor.

This equipment shall be connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.

This equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same DC supply circuit and the earthing conductor, and also the point of earthing of the DC system. The DC system shall not be earthed elsewhere.

The DC supply source is to be located within the same premises as this equipment.

Switching or disconnected devices shall not be in the earthed circuit conductor between the DC source and the point of the connection of the earthing electrode conductor.

CAUTION:

Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling Spectracom equipment.

CAUTION:

Once power is applied to the unit, DO NOT disconnect power unless the HALT command is first issued to the NetClock. Refer to Product Configuration for information on issuing the HALT command.

1) If desirable, install the rack-mount ears on the two sides of the front panel and install the unit in a standard 19 inch rack cabinet.

2) Connect the NetClock's front panel Ethernet port to an available hub/switch on the network with a standard network cable.

3) Connect the DC power input jack to a standard AC outlet with the supplied power supply. Verify the green Good Link lamp next to the Ethernet connector illuminates.

4) From the network administrator, obtain an available static network IP address, the network subnet mask and the IP address of the immediate gateway (if installed) if the subnet must access the NetClock. This step is only necessary if you are not using DHCP.

5) Assign the IP address, net mask and gateway settings by using the rear panel Serial Setup Interface DB9F connector interfaced to a PC with the provided serial cable (PC should be running either Microsoft HyperTerminal or ProComm). (Refer to *Options* for more information). This step is only necessary if you are not using DHCP.

6) Install the GPS antenna, surge suppressor, antenna cabling and GPS preamplifier if required. If using a window-mount antenna (Model 8228), place the antenna in a window that has no metallic tinting or screening in or on the glass and then place the unit in single-satellite mode.

NOTE: The 9300 Series NetClock must be in position hold if the unit is to use a window-mount GPS antenna. Position hold can be obtained by manually entering the GPS location or by receiving qualified GPS signal from at least four satellites at least once for a brief duration.

7) Connect the GPS cable to the rear panel antenna input jack on the back of the NetClock.

8) Verify the NetClock front panel Sync lamp illuminates green. Synchronization may take up to 20 minutes (approximately). It may take another 20 to 30 minutes for NTP to synchronize in turn. Individual networked devices will not be able to synchronize until NTP does.

9) If supplied with Option 03 Dial-out Modem, connect the dial-out modem to the rear panel Setup port. Change the console/client mode of operation to Modem using the Web User Interface.

10) Configure the NetClock front panel LCDs as desired using the Web User Interface.

11) Interface the NetClock to wall display clocks and other peripheral devices as needed.

12) Configure each of the rear panel outputs to these devices for desired local times, baud rates and Data Formats using either the Web User Interface or the serial setup port (Each port is separately configured so each port used may need to be configured for your desired configuration). If using a 9388 unit, configure the data formats to match.

NOTE: Unless you are using DNS in conjunction with DHCP (with the client configured using the NTP server's hostname instead of IP address), DHCP must be disabled and the IP address must be changed to a static address once the NetClock is properly configured. Failure to do this will result in a loss of time synchronization if the DHCP server assigns a new IP address to the NetClock. Verify your setup before synchronizing the network PCs via NTP.

13) Synchronize the network PCs via NTP using the Ethernet port as desired. (Refer to www.spectracomcorp.com for assistance and refer to Table 2-1 for information regarding local time.)

14) Review your security configuration settings.

Data Output	Port Available From	Time Zone Offset for Local Time	Automatic Daylight Saving Time Adjustment Capable	Additional Notes
Network Time Protocol (NTP)	Ethernet port on front panel	NOT AVAILABLE	NO	NTP is always UTC. Must set Local time/DST correction on each PC via the Date/Time properties window.
Data Format 0	Remote/Serial on rear panel	00-23 Hours	YES	None
Data Format 1	Remote/Serial on rear panel	+/-12:00	YES	None
Data Format 2	Remote/Serial on rear panel	NOT AVAILABLE	NO	Data Format 2 always reflects UTC. It can't be configured as local time.
Data Format 3	Remote/Serial on rear panel	+/-12:00	YES	None
Data Format 4	Remote/Serial on rear panel	NOT AVAILABLE	NO	Data Format 4 always reflects UTC. It can't be configured as local time.
Data Format 5	Remote/Serial on rear panel	+/-12:00	YES	None
Data Format 7	Remote/Serial on rear panel	NOT AVAILABLE	NO	Data Format 7 always reflects UTC. It can't be configured as local time.
Data Format 8	Remote/Serial on rear panel	00-23 Hours	YES	None
Data Format 90	Remote/Serial on rear panel	NOT AVAILABLE	NO	Data Format 90 always reflects UTC. It can't be configured as local time.
IRIG B	IRIG port on rear panel	+/-12:00	YES	None
IRIG E	IRIG port on rear panel	+/-12:00	YES	None

Table 2-1: Time Zone Offsets available for Data Outputs

2.3 Required Tools and Cables

1) Phillips screwdriver to install the unit's rack-mount ears.

2) Screwdriver to mount the unit in a standard 19-inch rack.

3) Wire strippers for the RS-485 cabling.

4) Supplied jeweler's type screwdriver for tightening the RS-485 wiring terminal block connectors (Located in the ancillary kit).

5) RS-232 straight-thru DB9 to DB9 cable (supplied)

6) Ethernet cables (Refer to Section 2.7).

2.4 Power and Ground Connection

WARNING:

This equipment has a connection between the earthed conductor of the DC supply circuit and the earthing conductor.

This equipment shall be connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.

This equipment shall be located in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same DC supply circuit and the earthing conductor, and also the point of earthing of the DC system. The DC system shall not be earthed elsewhere.

The DC supply source is to be located within the same premises as this equipment.

Switching or disconnected devices shall not be in the earthed circuit conductor between the DC source and the point of the connection of the earthing electrode conductor.

CAUTION:

Electronic equipment is sensitive to Electrostatic Discharge (ESD). Observe all ESD precautions and safeguards when handling Spectracom equipment.

An external AC to DC power adapter powers the NetClock.

This International and US Desk Top adapter has a detachable AC power cord to an IEC 320 connector. The power adapter is shipped with a line cord compatible with AC receptacles (NEMA 5-15R) commonly found in the United States and Canada. Alternate type line cords or adapters may be obtained locally.

The chassis ground stud allows the NetClock chassis to be connected to an earth ground or single point ground. Connecting the chassis to a single point ground system may be required in some installations to ensure optimum lightning protection. An earth ground is also recommended in installations where excessive noise on the power line degrades receiver performance.

Rack-mount ears are provided in the ancillary kit if the NetClock will be installed in a standard 19 inch rack.

2.5 Rack Mounting

To rack-mount the unit, locate the rack-mount ears. Using the rack mounting screws provided in the ancillary kit (refer to 2.1, *Inventory*), mount the ears to the sides of the unit. (If the NetClock is to be mounted flush with the front of the rack, mount the ears to the front of the unit.) Slide the unit into the rack and connect the ears to the rack using appropriate screws (not provided).

2.6 GPS Antenna Installation

2.6.1 Antenna Cable for Outdoor Antenna

When using the Model 8225 GPS outdoor antenna, Spectracom recommends using LMR-400 low loss type cable for the GPS antenna cable. To simplify the installation process, Spectracom offers GPS cable assemblies terminated with Type N Male connectors. Standard lengths are 10, 25, 50, 100, 150 and 200 feet.

If the antenna cable is purchased locally, select coax suitable for outdoor use. Consider the cable's weather ability, temperature range, UV resistance, and attenuation characteristics.

Do not allow the antenna cable to be placed in standing water, as water may permeate through the coax jacket over time. On flat roof installations, the coax can be suspended by cable hangers or placed in sealed PVC conduit. Apply a weather proofing sealant or tape over all outdoor connections.

Installation of a surge protection device in the antenna line is recommended to protect the NetClock receiver and connected devices from lightning damage. Spectracom offers the Model 8226 Impulse Suppressor to shunt potentially damaging voltages on the antenna coax to ground. Refer to the Model 8226 Impulse Suppressor Section for a complete description of the Model 8226.

2.6.2 Cable Lengths

The maximum recommended antenna cable length when installed without a preamplifier is 300 feet of LMR 400 or equivalent cable with a maximum attenuation (loss) of 16 dB (Figure 2-1).

When selecting alternate antenna cable sources, the attenuation characteristics at the GPS frequency of 1575.42 MHz must be known. To ensure optimum receiver performance, the total antenna cable attenuation must not exceed 16 dB regardless of cable length. Cable attenuation of greater than 16 dB requires the use of a Model 8227 Inline Amplifier (Figure 2-2).

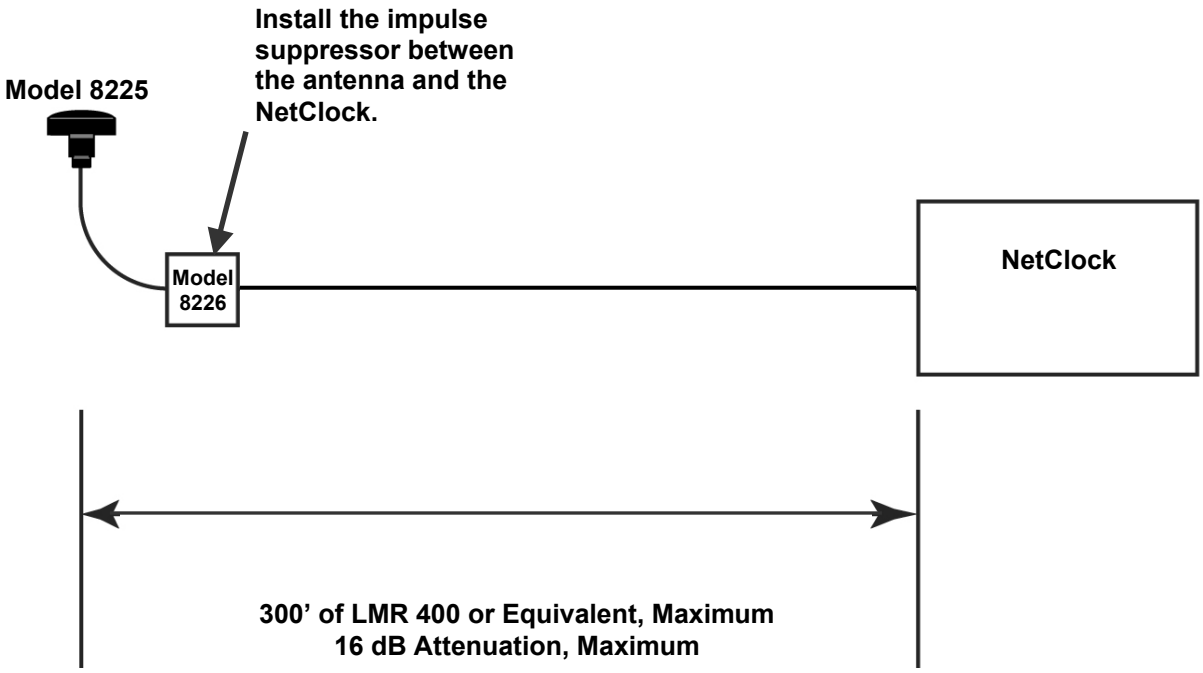

Install the impulse suppressor between the antenna and the NetClock.
Model 8225
Model 8226
NetClock
300' of LMR 400 or Equivalent, Maximum
16 dB Attenuation, Maximum

Figure 2-1: Cabling without Inline Amplifier

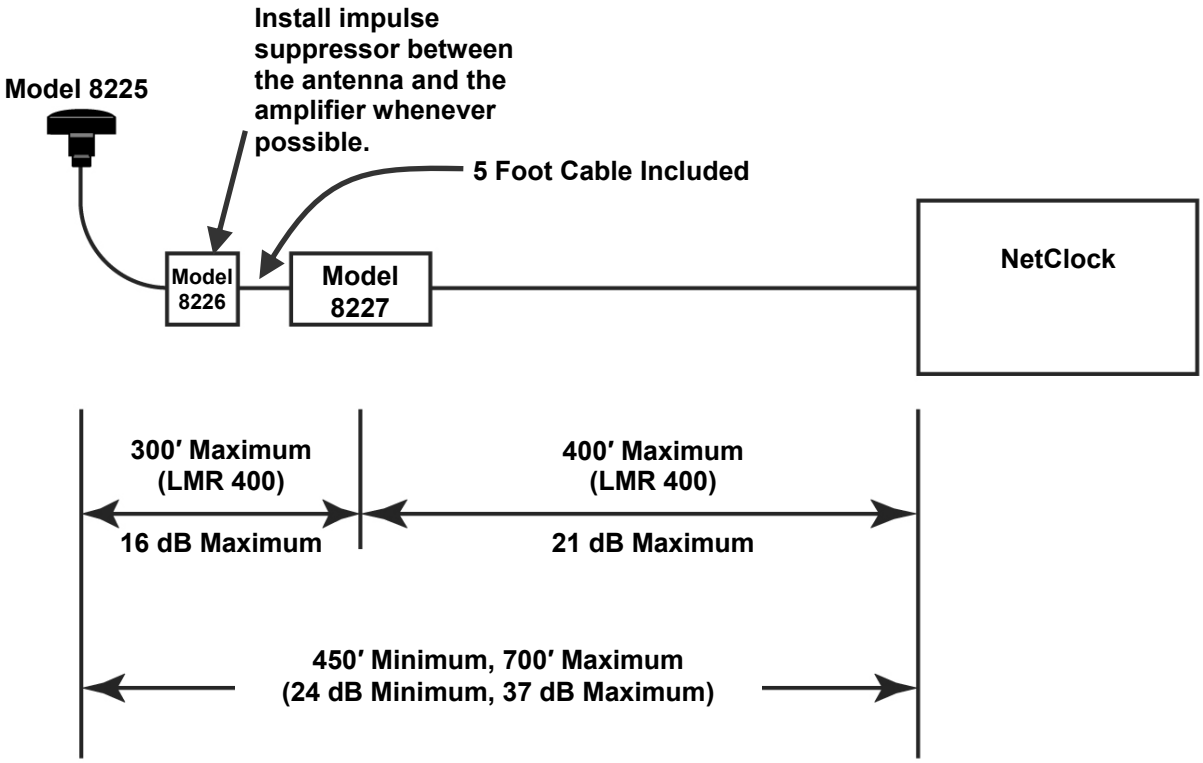


Figure 2-2: Cabling with Inline Amplifier

2.6.3 Model 8224 GPS Splitter

The GPS Antenna Splitter, Model 8224, is designed for use with an existing antenna/cable setup. It eliminates the need and expense for a second antenna/cable run when two synchronization systems are desirable. The Model 8224 should be installed indoors.

2.6.4 Model 8226 Impulse Suppressor

Spectracom recommends the use of an inline coaxial protector for all products with an outside antenna. Spectracom offers the Model 8226, Impulse Suppressor, to protect the receiver from damaging voltages occurring on the antenna coax. Voltages exceeding the impulse suppresser trip point are shunted to the system ground. The Model 8226 is designed to withstand multiple surges.

Two LMR-400 field-installable N type connectors are provided with the Model 8226 to splice in the surge suppressor wherever it must be placed. However, the recommended method to avoid having to cut the antenna cable is to determine the desired location of the Model 8226 ahead of time and then order two lengths of pre-terminated cables instead of just one long cable that spans the entire distance between the antenna and the NetClock.

Mount the suppressor indoors, preferably where the coax enters the building. Install the suppressor on a grounding panel or bulkhead as shown in Figure 2-3.

Spectracom offers a grounding kit that includes grounding cable, clamps, mounting bracket and ground plane. The Spectracom Part Number for this kit is 8226-0002-0600. Contact our Sales department for additional information.

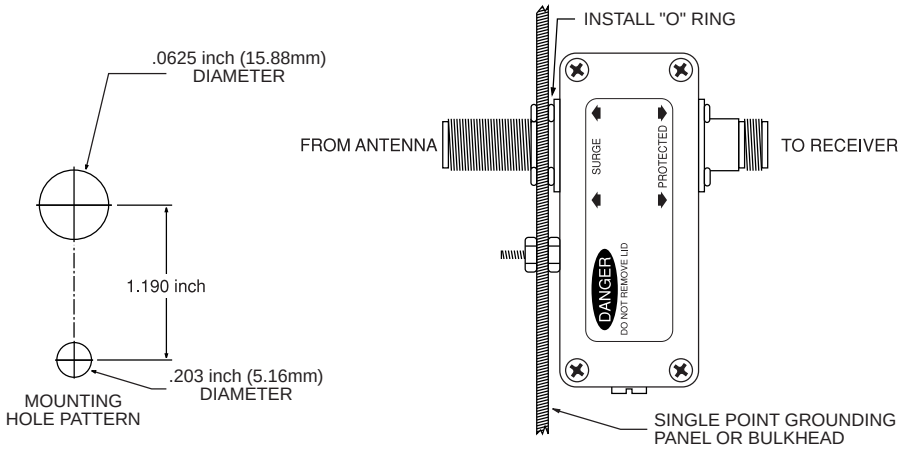


Figure 2-3: Model 8226 Impulse Suppressor

Refer to the Model 8226 Manual for proper installation.

2.6.5 Model 8227 GPS Inline Amplifier

An inline amplifier is required whenever GPS antenna cable lengths cause greater than 16 dB attenuation.

The Model 8227 GPS Inline Amplifier, shown in Figure 2-3, extends the maximum cable length. The Model 8227 provides 20 dB of gain and is powered by the NetClock receiver.

Figure 2-4: Model 8227 Inline Amplifier

Two LMR-400 field-installable N type connectors are provided with the Model 8227 to splice in the amplifier wherever it must be placed. However, the recommended method to avoid having to cut the antenna cable is to determine the desired location of the Model 8227 ahead of time and then order two lengths of pre-terminated cables instead of just one long cable that spans the entire distance between the antenna and the NetClock.

A five foot N type connector cable is also supplied with the Model 8227 to allow it to be installed after the Model 8226 surge suppressor. The Model 8227 should always be installed after the surge suppressor to prevent lightning or surge damage to the preamp.
Refer to the Model 8227 Manual for proper installation.

2.7 Ethernet Network Cabling

Spectracom NetClocks provide a 10/100 Ethernet port for full NTP functionality as well as full web browser user interface enabled configuration, monitoring and diagnostic support.

The Ethernet port is provided on the front panel for easy connection to routers and hubs.

Use standard CAT 5 cable with RJ45 connectors.

When connecting to a hub or router use a straight-through wired cable.

When connecting directly to a PC, use a crossover wired cable.

2.7.1 Optional CNC3000 Cable Kit

Spectracom offers an available cable kit called the CNC3000. This kit consists of three cables:

1) Six foot RS-232 Setup port cable DB9M to DB8F for initial configuration
1) Six foot Cat 5 crossover LAN cable for direct PC connection
1) Six foot Cat 5 patch LAN cable for LAN hub link.

Contact our Sales department if you would like to obtain the CNC3000 kit.

2.8 Remote Port and Serial Comm Port Output Pin-outs and Wiring

This section contains wiring and pin-out information for the rear panel Remote RS-485 and Serial RS-232 Comm ports.

2.8.1 Serial Comm Ports

The rear panel of the 9300 Series has two RS-232 SERIAL COMM ports that are available to synchronize peripheral devices. These ports can provide RS-232 output data to synchronize external devices that can accept RS-232 Data Formats as an input.

The Serial Ports can provide RS-232 data in one of two modes. The Interrogation mode provides a one-time RS-232 time stamp each time that the port receives a request character from the external device. In between the requests for time, there is no output. The Multicast mode broadcasts the time stamp every second. The Interrogation mode is the factory default. This mode should be changed to Multicast mode in the web browser user interface if the external device being synchronized does not send a request character for the time but rather just “listens” for the time to be sent every second.

The configuration of the data, including the baud rate, the Data Format, the request character in the Interrogation mode, Time Zone Offsets and Daylight Saving Time rules is chosen from the web browser user interface.

The Serial Ports have a standard RS-232 pin configuration as shown in Figure 2-5 and Table 2-2.

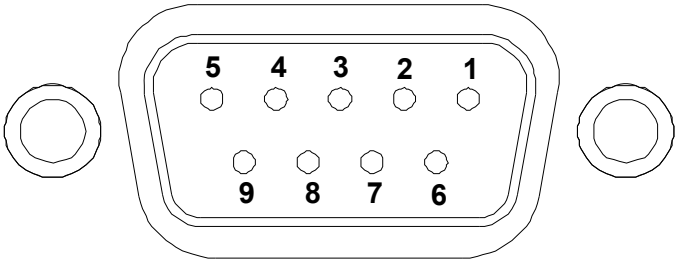


Figure 2-5: Serial Port Pin Configuration

PIN	SIGNAL	I/O	DESCRIPTION
2	RXD	O	Receive Data (RS-232 output data to a device)
3	TXD	I	Transmit Data (RS-232 input data from a device)
5	GND	-	Signal Common
6	DSR	O	Data Set Ready
7	RTS	*	Request to Send
8	CTS	*	Clear to Send

Table 2-2: Serial Port Pin Assignments

2.8.2 RS-485 Remote Port

The NetClock has two remote ports labeled “RS-485 PORT 1” and “RS-485 PORT 2”. These outputs provide a continuous once-per-second time data stream in the selected Data Format. Two input time Data Formats, five output time Data Format selections, and one position data stream in NMEA 0183 format are available. Refer to Section 6 for a complete description of the Data Format structures.

In addition to Data Formats, baud rate and UTC time difference of each output is selectable.

A 3-position terminal block is supplied in the ancillary kit for each of the Remote Connections. Also included in the ancillary kit is a jeweler’s type screwdriver to tighten the screws. Connector pin assignments are shown in Figure 2-6.

Figure 2-6: Remote Outputs

RS-485 is a balanced differential transmission requiring twisted pair cabling.

RS-485 characteristics make it ideal to distribute time data throughout a facility. Each Remote Output can provide time to 32 devices at cable lengths up to 4,000 feet. Refer to the RS-485 Output diagram for a schematic representation of each RS-485 output driver. Relative to RS-485 specifications, the A terminal (Pin 2) is negative with respect to the B terminal (Pin 1) for a mark or binary 1. The A terminal is positive to the B terminal for a space or binary 0.

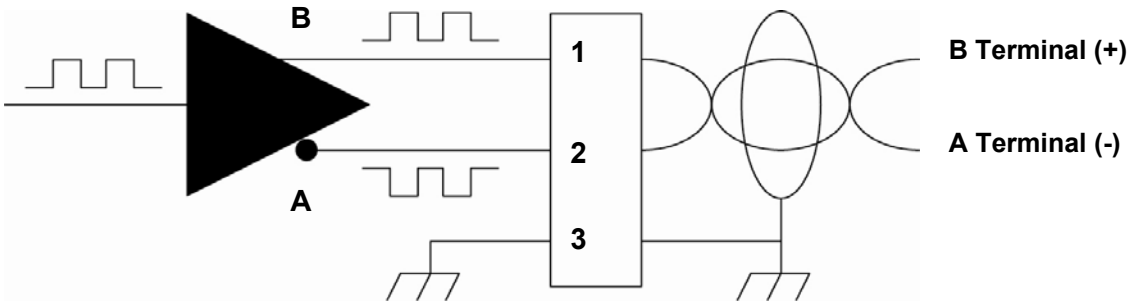


Figure 2-7: RS-485 Output

Spectracom offers many devices that accept the RS-485 data stream as an input reference. These products include display clocks, RS-485 to RS-232 converters, Ethernet Time Servers, and radio link products to meet various time applications and requirements. For information on Remote Output usage refer to Section 2.8.2.

2.8.3 Remote Output Usage

The Remote Outputs provide a continuous once-per-second time data stream in RS-485 levels. RS-485 is a balanced differential transmission, which offers exceptional noise immunity, long cable runs and multiple loading. These characteristics make RS-485 ideal for distributing time data throughout a facility.

Each Remote Output can drive 32 devices over cable lengths up to 4000 feet. Spectracom manufactures wall clocks, Ethernet Time Servers, RS-485 to RS-232 converters and radio link products that utilize the RS-485 data stream as an input.

Refer to sections 2.8.4, 2.8.5, and 2.8.6 for more information on time data bus interconnections. Follow the guidelines contained therein when constructing the RS-485 data bus.

2.8.4 RS-485 Guidelines and Cable Selection

Low capacitance, shielded twisted pair cable is recommended for installations where the RS-485 cable length is expected to exceed 1500 feet. Table 2-3 suggests some manufacturers and part numbers for extended distance cables. These cables are specifically designed for RS-422 or RS-485 applications; they have a braided copper shield, nominal impedance of 120 ohms, and a capacitance of 12 to 16 picofarads per foot.

RS-485 cable may be purchased from Spectracom. Specify part number CW04xxx, where xxx equals the length in feet.

MANUFACTURER	PART NUMBER
Belden Wire and Cable Company 1-800-BELDEN-1	9841
Carol Cable Company 606-572-8000	C0841
National Wire and Cable Corp. 232-225-5611	D-210-1

Table 2-3: Cable Sources for RS-485 Lines Over 1500 Feet

For cable runs less than 1500 feet, a lower-cost twisted pair cable may be used. Refer to Table 2-4 for possible sources. In addition, Category 5 cables may be used for cable runs less than 1500 feet.

MANUFACTURER	PART NUMBER
Alpha Wire Corporation 1-800-52ALPHA	5471
Belden Wire and Cable Company 1-800-BELDEN-1	9501
Carol Cable Company 606-572-8000	C0600

Table 2-4: Cable Sources for RS-485 Lines Under 1500 Feet

2.8.5 Connection Method

The RS-485 transmission line must be connected in a daisy chain configuration as shown in Figure 2-8. In a daisy chain configuration, the transmission line connects from one RS-485 receiver to the next. The transmission line appears as one continuous line to the RS-485 driver.

A branched or star configuration is not recommended. This method of connection appears as stubs to the RS-485 transmission line. Stub lengths affect the bus impedance and capacitive loading which could result in reflections and signal distortion.

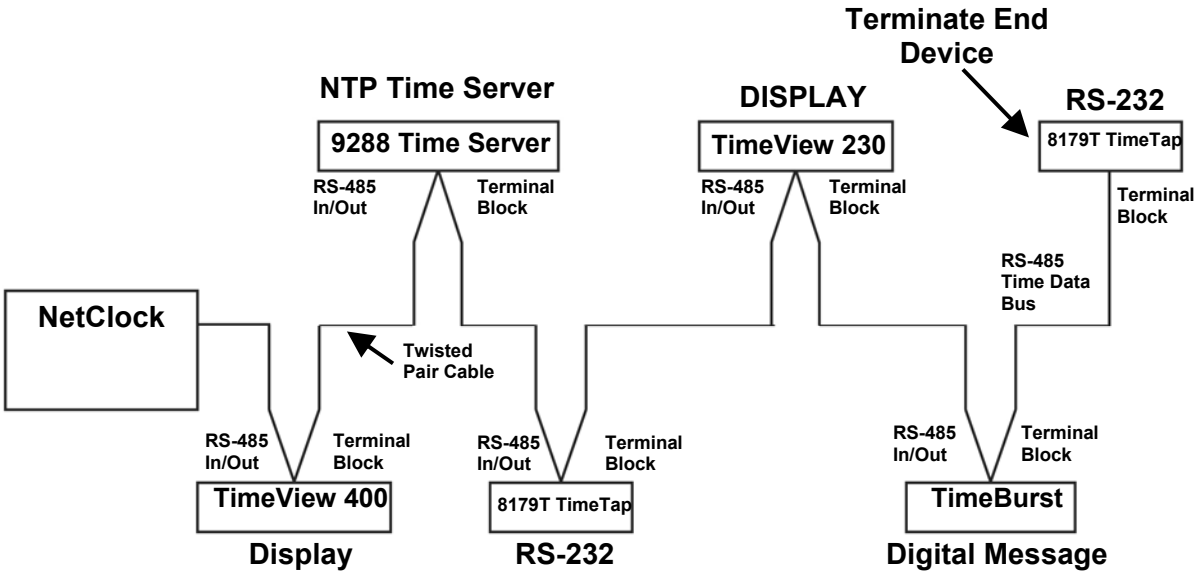


Figure 2-8: One-Way Bus Installation

The RS-485 Output can be split in a total of two directions as shown in Figure 2-9. This allows the NetClock to be centrally located. Connecting in this method can simplify installation and possibly reduce the amount of cable required.

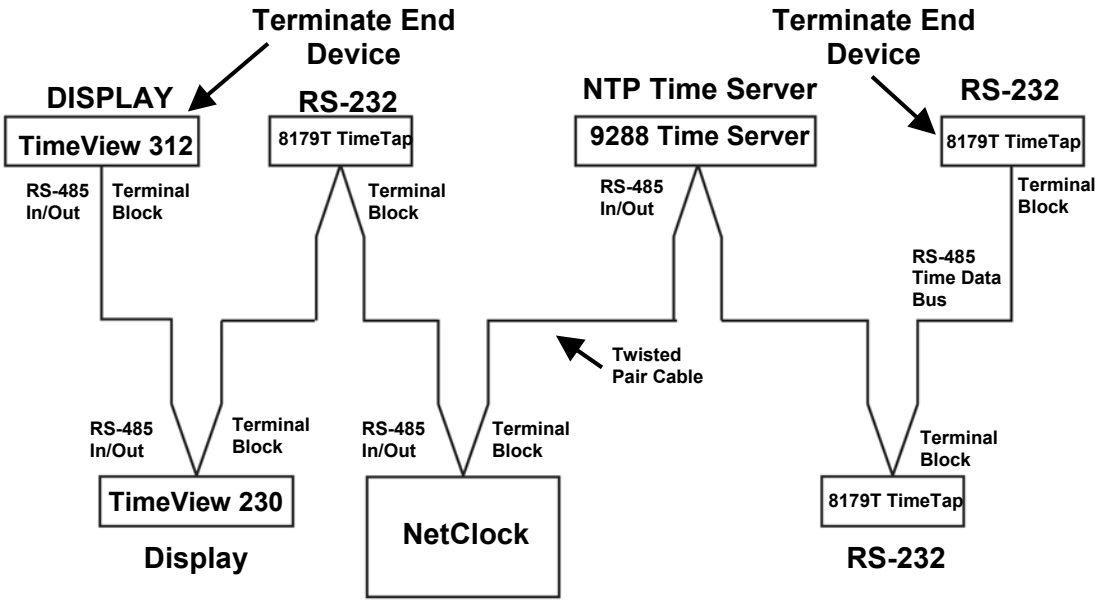


Figure 2-9: Split Bus Configuration

NOTE: Most RS-485 connections found on Spectracom equipment are made using a removable terminal strip. A jaw that compresses the wires when tightened secures the wires. When using small diameter wire, 22-26 gauge, a strain relief can be fashioned by wrapping the stripped wire over the insulating jacket. Wrapping the wires in this manner prevents smaller gauge wires from breaking off when exposed to handling or movement.

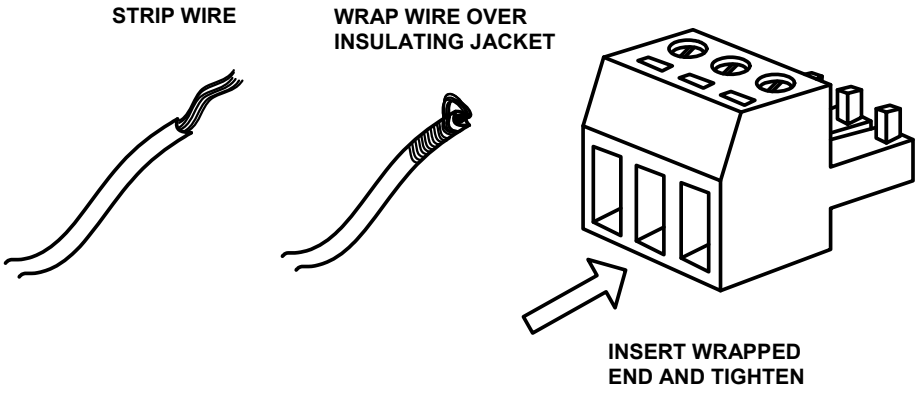


Figure 2-10: Wire Strain Relief

TimeView display clocks use a 6-position terminal block to connect to the RS-485 data bus. Connect the TimeView to the NetClock RS-485 Output as shown in
Figure 2-11. The TimeView display clocks accept only Data Formats 0 or 1.

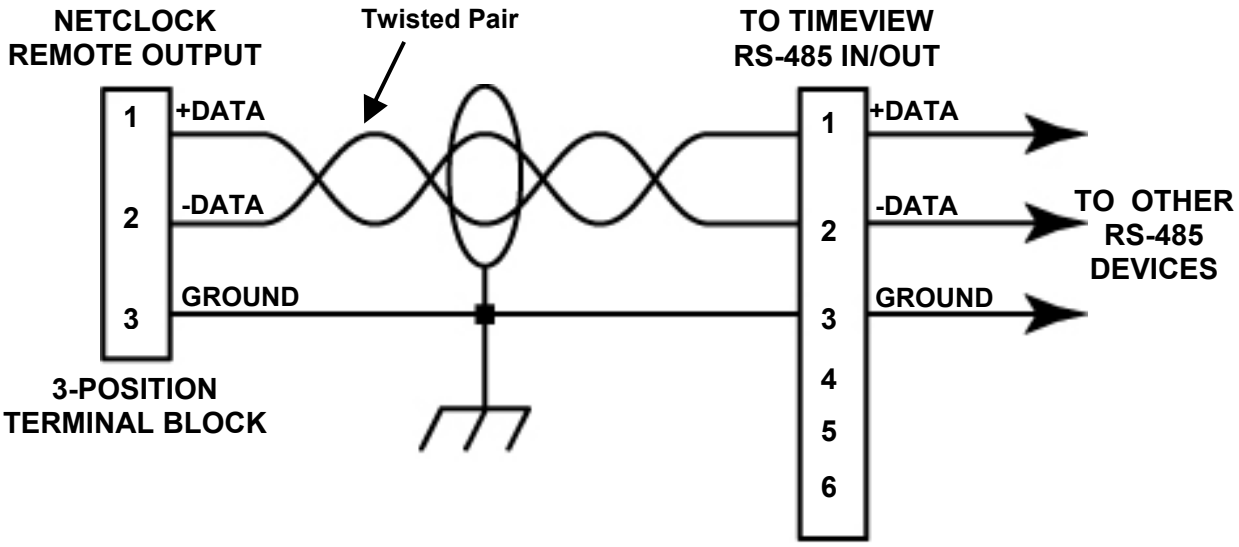


Figure 2-11: TimeView RS-485 Interface

The Model 8179T TimeTap is an RS-485 to RS-232 converter. The Model 8179T has a DB9 RS-232 interface that receives operational power from the RS-232 flow control pins RTS or DTR. Connect the TimeTap to the RS-485 data bus as shown in Figure 2-12.

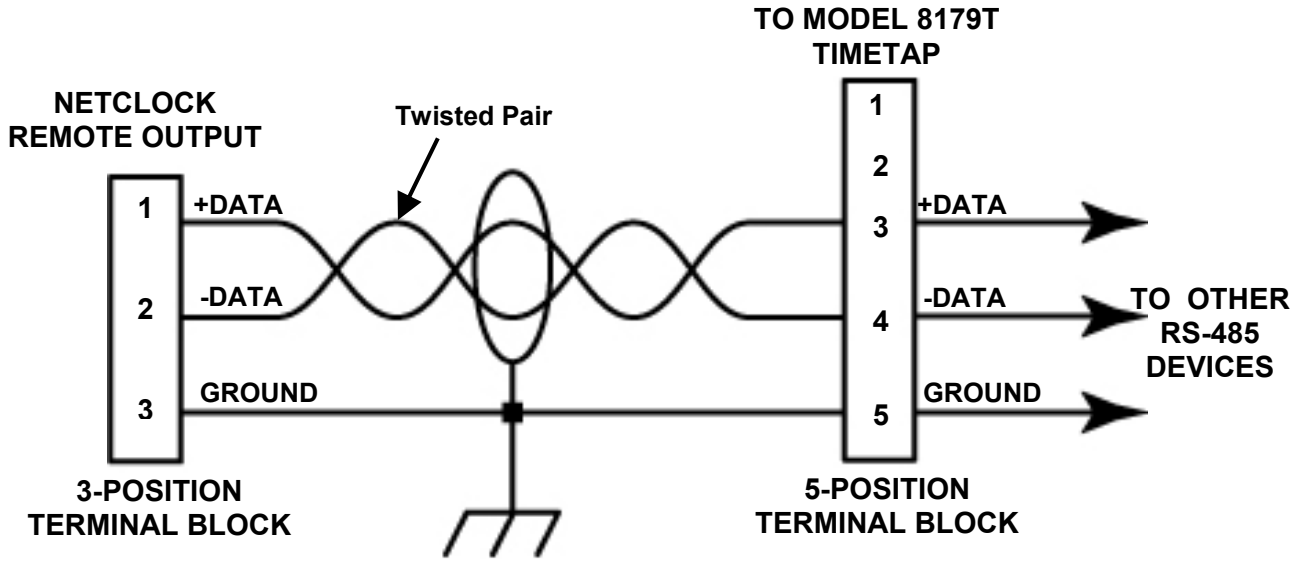


Figure 2-12: Model 8179T TimeTap RS-485 Interface

Spectracom Model 9288 is an Ethernet Time Server that supports NTP and SNTP time protocols. The Model 9288 accepts Format 0, Format 2, Format 7, or Format 8 (Formats 7 and 8 are not available on all time sources – Contact Tech Support for additional information) and connects to the RS-485 data bus through a three-position terminal block. Connect the Model 9288 to the NetClock as shown in Figure 2-13.

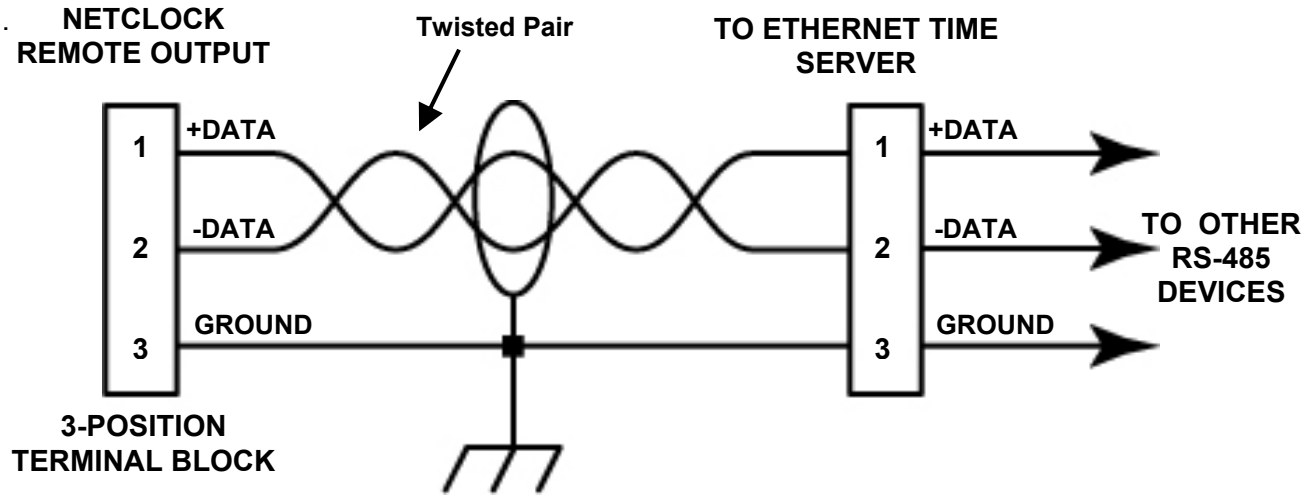


Figure 2-13: Model 9288 RS-485 Interface

The Model 8185, TimeBurst™, provides a digital time-of-day data burst to a radio transmitter. The TimeBurst accepts Data Format 0 or 1. Connect the TimeBurst to the RS-485 data bus using a 3-position terminal block as shown in Figure 2-14.

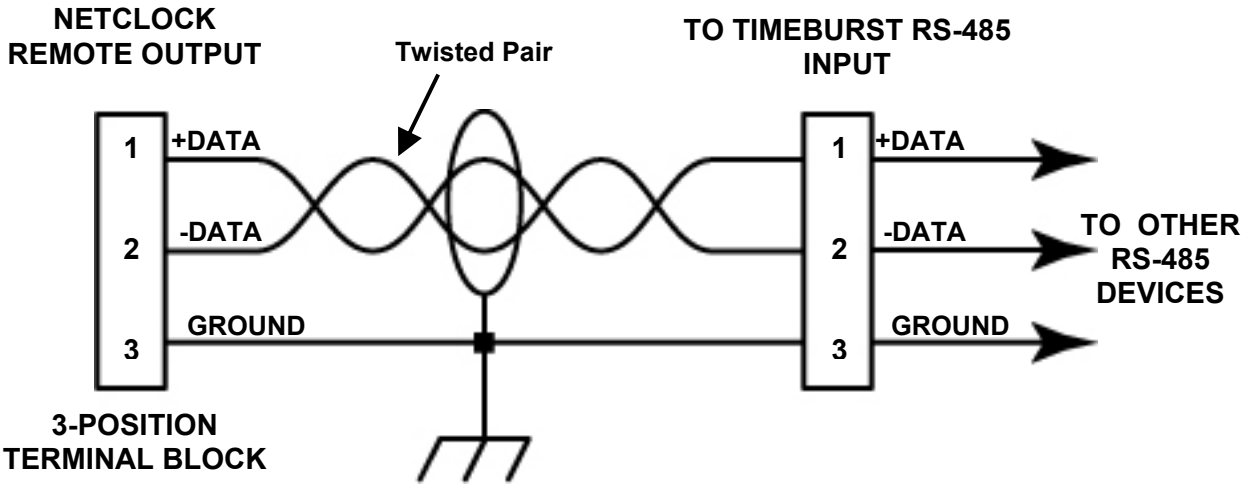


Figure 2-14: TimeBurst RS-485 Interface

2.8.6 Termination

A 120 Ohm termination resistor is required on devices located at the ends of the RS-485 transmission line. Terminating the cable end preserves data integrity by preventing signal reflections.

For a one-way bus installation (Figure 2-8), terminate the last device on the bus. The RS-485 data bus can be split in two directions as shown in Figure 2-9. In a split bus configuration, terminate the devices installed on each end of the bus. Some Spectracom products include a built-in termination switch to terminate the RS-485 bus when required or a resistor is supplied with the equipment if no termination switch is available. The terminating resistor is installed between the positive and negative connections on the terminal block of the last RS-485 connection.

3 Product Configuration

NOTE: Screens shown in this manual are for illustrative purposes. Actual screens may vary. Software common to multiple NetClock models may be used to generate these screens. As a result, labels in the screens displayed may refer to units other than your specific NetClock. Software operation should be common among these models, where appropriate.

After installing the NetClock, verify that power is connected and wait for the device to boot up.

The front panel display provides certain configuration data on start-up. The right panel, by factory default, displays the date and time (UTC). The left panel displays the unit's hostname, IPv4 address, mask, and gateway.

NOTE: If using DHCP, the IP address will be assigned automatically and displayed on the front panel. You may use a Web browser to connect to this IP address and configure the NetClock through the Web Browser User Interface (Web UI) (Figure 3-1). *Refer to Network Configuration with DHCP*, Section 3.1.

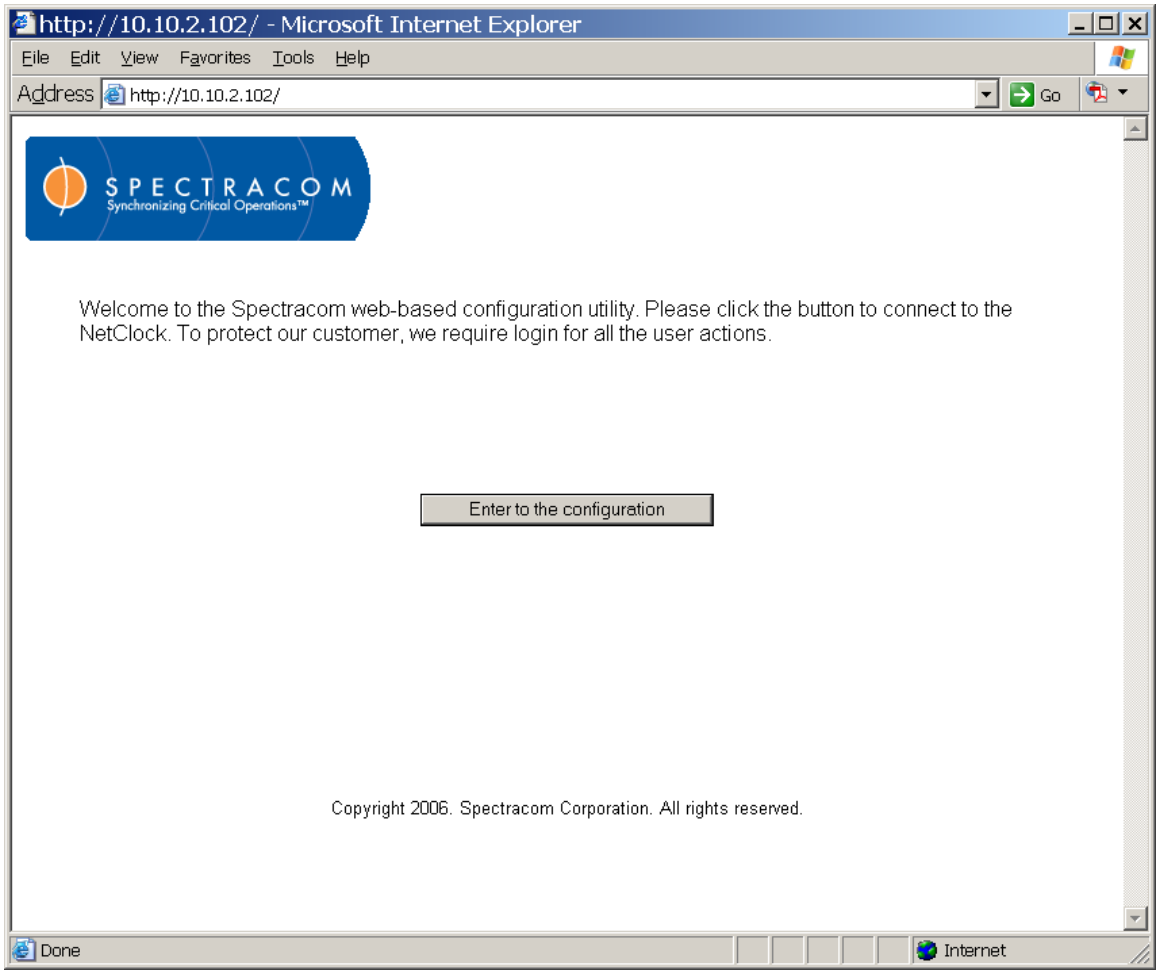

http://10.10.2.102/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/
Go
SPECTRACOM
Synchronizing Critical Operations™
Welcome to the Spectracom web-based configuration utility. Please click the button to connect to the NetClock. To protect our customer, we require login for all the user actions.
Enter to the configuration
Copyright 2006. Spectracom Corporation. All rights reserved.
Done
Internet

Figure 3-1: Entering to the Configuration in the Web UI

When configuring a NetClock without DHCP, or to configure a NetClock that has not been assigned an IP address, refer to *Network Configuration*, Section 3.2.

3.1 Network Configuration with DHCP

Once connected to the DHCP server through the network, the NetClock is assigned an IP address. This address and other network information is displayed on the front panel when the device boots up. Enter the IP address in your browser (on a computer connected to the network) and log in as an administrator. The http session will be redirected automatically to an https session and a security certificate pop-up window will be displayed. Accept the certificate by clicking "OK."

*Your login name is **admin***
*The password is **admin123***

NOTE: Unless you are using DNS in conjunction with DHCP (with the client configured using the NTP server's hostname instead of IP address), DHCP must be disabled and the IP address must be changed to a static address once the NetClock is properly configured. Failure to do this will result in a loss of time synchronization if the DHCP server assigns a new IP address to the NetClock.

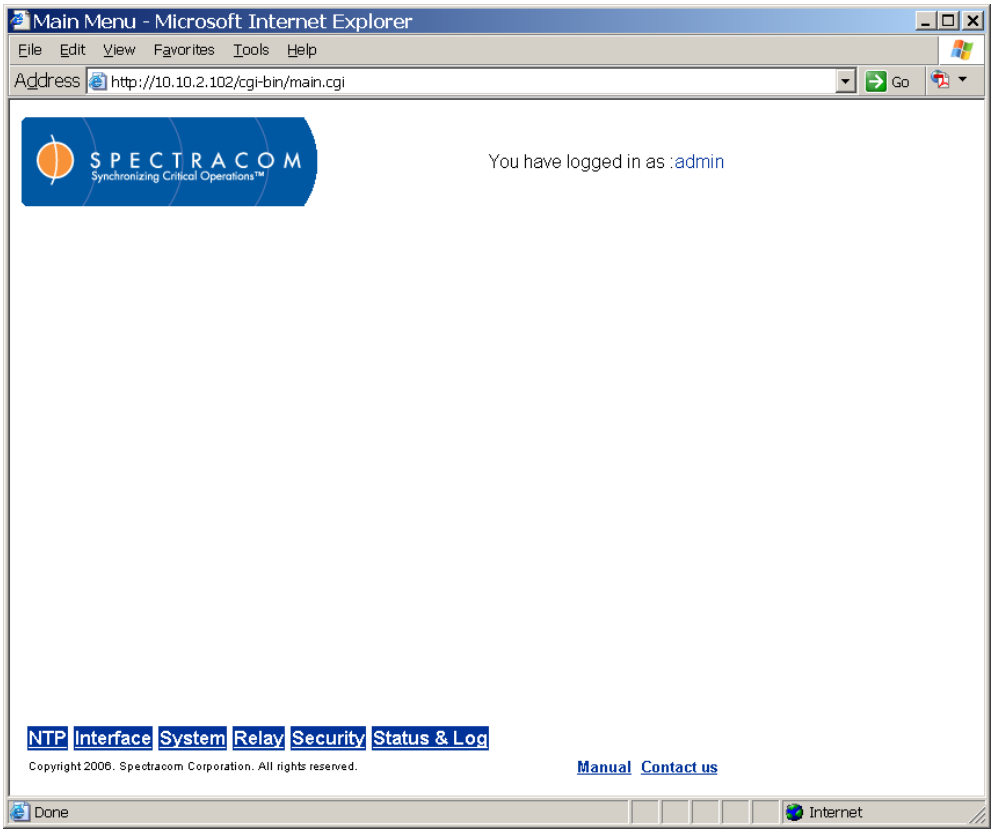


Figure 3-2: Web Browser User Interface (Web UI)

When you enter the NetClock IP address in your browser (this will differ from the IP address shown in the examples within this manual), you will be prompted to log in (Figure 3-1). The default administrator account is set at the factory as **admin**. The password is **admin123**.

After entering the login name and password and successfully logging into the NetClock, the user will see a Web UI screen similar to Figure 3-2. From this screen, click the Security tab. The Security menu will be displayed on the left side of the Web UI. Click the Network link to access the necessary Network configuration fields (Figure 3-3 and Figure 3-4).

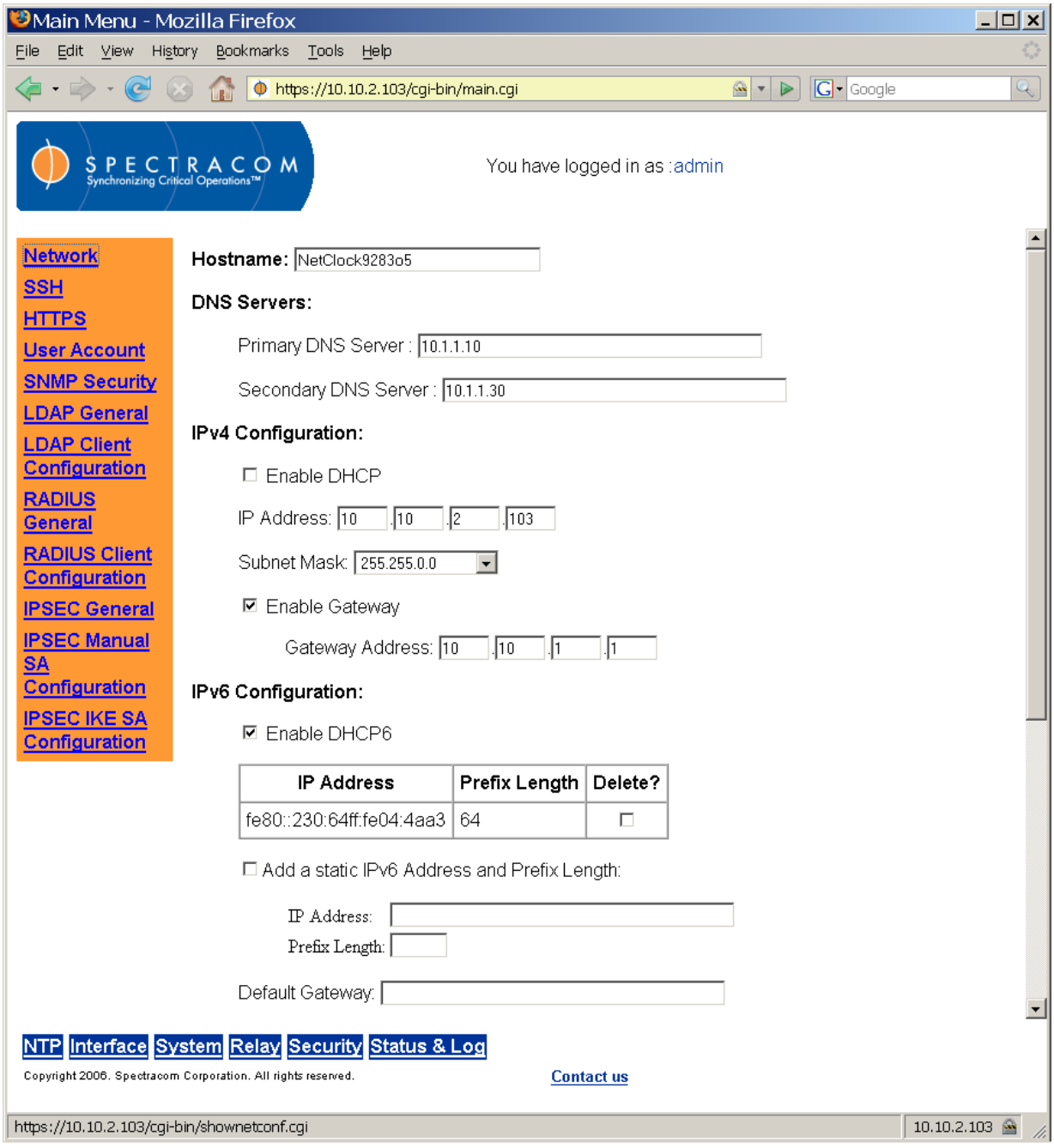


Figure 3-3: Security – Network Screen (1 of 2)

Refer to the *Initial Network Configuration* section to continue your product configuration.

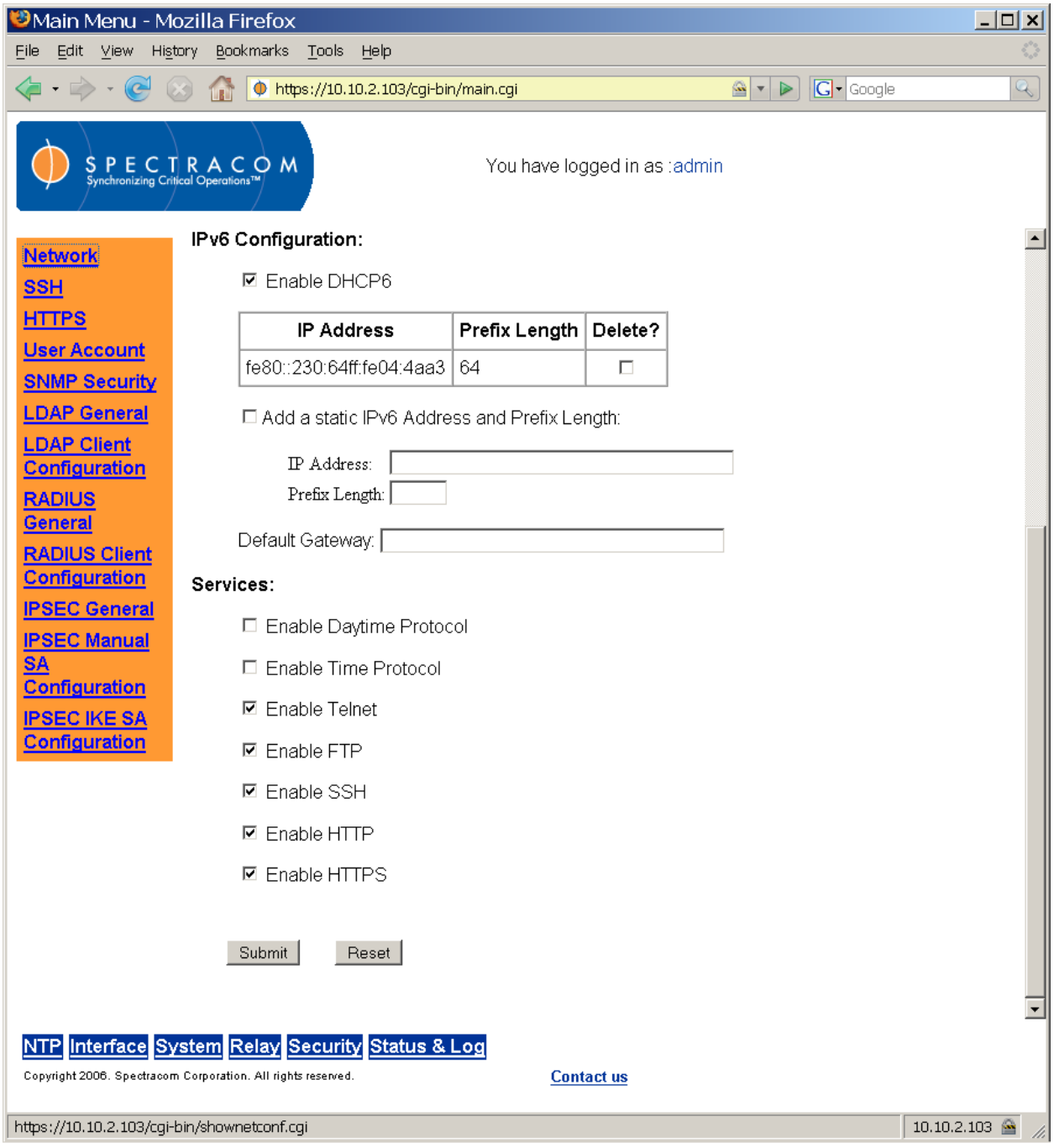


Figure 3-4: Security – Network Screen (2 of 2)

3.2 Initial Network Configuration

NOTE: The IP address assignment in this configuration may be performed even if your network has a DHCP server. There may be times when you do not wish DHCP to assign the IP address for the NetClock.

To configure a NetClock without DHCP or to configure a NetClock that has not been assigned an IP address, use the provided serial cable to connect a PC or laptop computer to the serial setup port on the back of the NetClock. After making this connection, use a terminal program (such as HyperTerminal) to log into the NetClock as an administrator. Use the Command Line Interface (CLI) in the terminal program to configure initial values and determine the NetClock's network address.

3.2.1 Using HyperTerminal to Connect to the NetClock

Microsoft's HyperTerminal program is typically located under *Accessories – Communications* in the Windows PC Start Menu. (Most terminal programs can be used to connect to the NetClock. it is not necessary to use HyperTerminal specifically.) Establish a new connection using the serial port to which you have connected the NetClock (typically COM1).

Figure 3-5: Establishing a New Terminal Connection

Figure 3-6: Connecting to the Computer's Serial Port

Configure the COM1 properties as shown in Figure 3-7. *Bits per second* should be **9600**. *Data bits* should be **8**. *Parity* should be **none**. *Stop bits* should be **1**. *Flow control* should be **none**. When the connection is established in the terminal window, the command line prompt will appear (Figure 3-8).

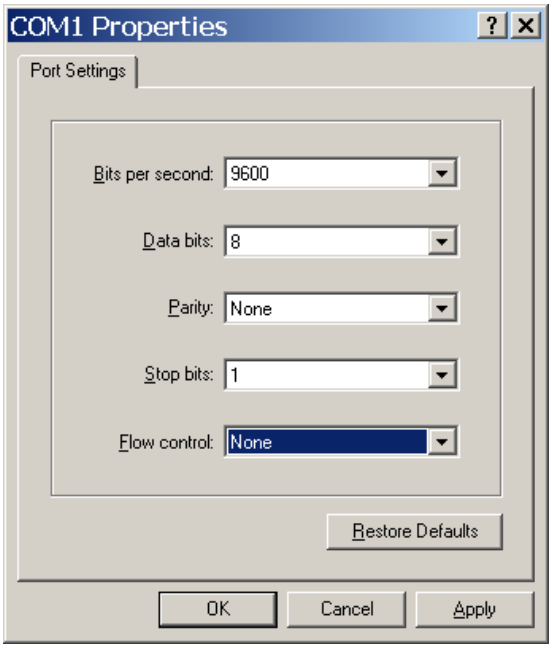


Figure 3-7: Configuring the Serial Port Connection Properties

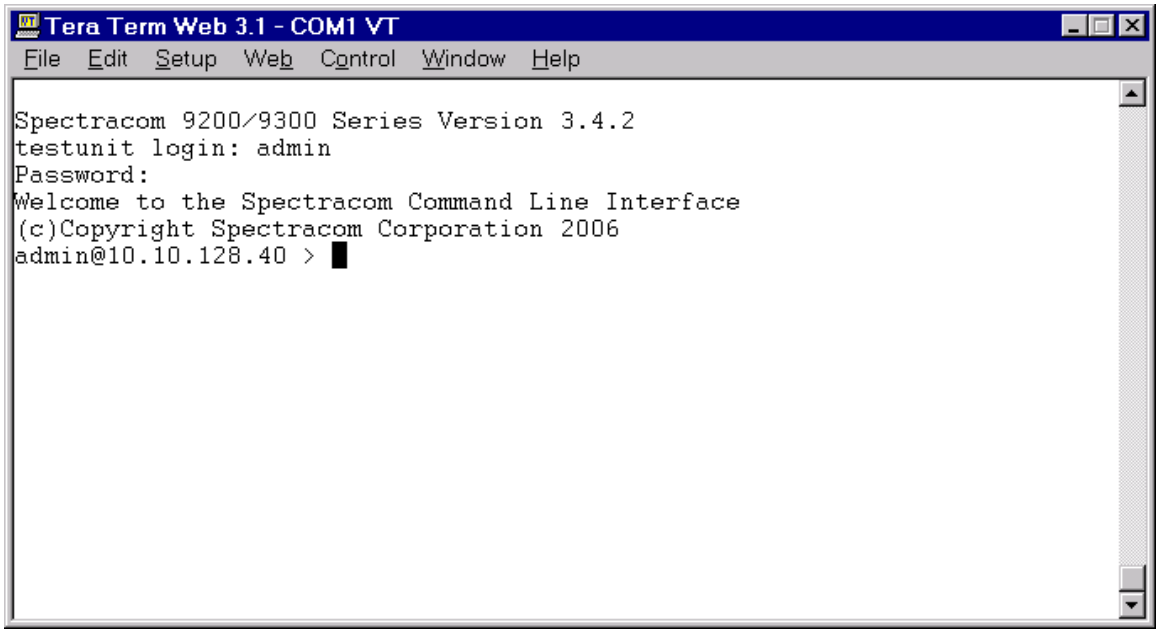

Tera Term Web 3.1 - COM1 VT
File Edit Setup Web Control Window Help
Spectracom 9200/9300 Series Version 3.4.2
testunit login: admin
Password:
Welcome to the Spectracom Command Line Interface
(c)Copyright Spectracom Corporation 2006
admin@10.10.128.40 >

Figure 3-8: Spectracom NetClock Command Line Interface (CLI)

Log in as an administrator using the name **admin** and the password **admin123**. (Login names and passwords are case-sensitive.) A successful login will return the prompt *admin@x.x.x.x*, where *x.x.x.x* is the IP address of the NetClock.

Typing **help** in the Command Line Interface (CLI) will display a list of available commands (Figure 3-9). Typing net will display the CLI net commands. The command **net config** will walk the user through initial configuration.

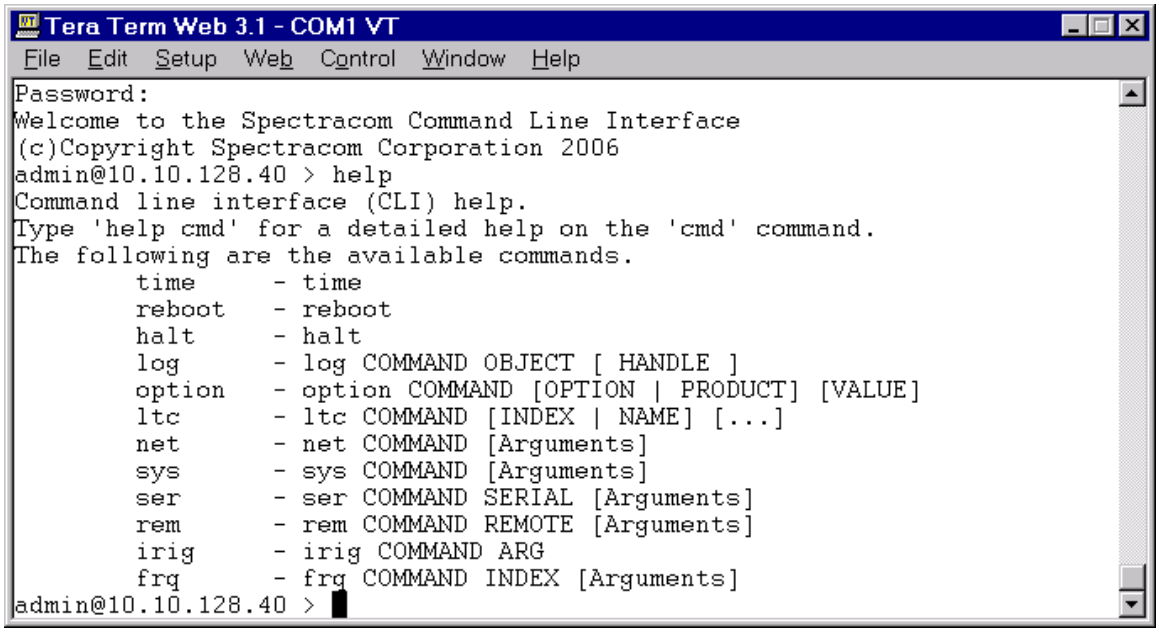

Tera Term Web 3.1 - COM1 VT
File Edit Setup Web Control Window Help
Password:
Welcome to the Spectracom Command Line Interface
(c)Copyright Spectracom Corporation 2006
admin@10.10.128.40 > help
Command line interface (CLI) help.
Type 'help cmd' for a detailed help on the 'cmd' command.
The following are the available commands.
time - time
reboot - reboot
halt - halt
log - log COMMAND OBJECT [HANDLE]
option - option COMMAND [OPTION | PRODUCT] [VALUE]
ltc - ltc COMMAND [INDEX | NAME] [...]
net - net COMMAND [Arguments]
sys - sys COMMAND [Arguments]
ser - ser COMMAND SERIAL [Arguments]
rem - rem COMMAND REMOTE [Arguments]
irig - irig COMMAND ARG
frq - frq COMMAND INDEX [Arguments]
admin@10.10.128.40 >

Figure 3-9: Available CLI Commands

Initial configuration settings can be modified subsequently through either the serial port or the Web UI. The values entered in the following fields are specific to your setup. Your network administrator may assign and provide some or all of the required information.

If you are not using DHCP in conjunction with DNS (using domain names rather than IP addresses), the IP address of the NetClock must be changed from the factory default to the new static address for your particular network before the NetClock can be accessed through the Web UI (and before it can provide NTP time stamps to synchronize the network).

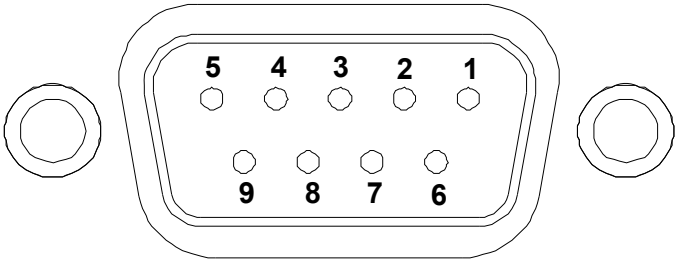


Figure 3-10: Serial Port Pin Configuration

PIN	SIGNAL	I/O	DESCRIPTION
2	RXD	O	Receive Data (RS-232 output data to PC)
3	TXD	I	Transmit Data (RS-232 input data from PC)
5	GND	-	Signal Common
6	DSR	O	Data Set Ready
7	RTS	*	Request to Send
8	CTS	*	Clear to Send

Table 3-1: Serial Setup Cable Pin-Outs

3.2.2 Initial Network Setup

At the CLI, enter the command **net config**. Set the prompted values to complete initial network setup. In this manual, the convention <enter> is used to indicate pressing the enter key.

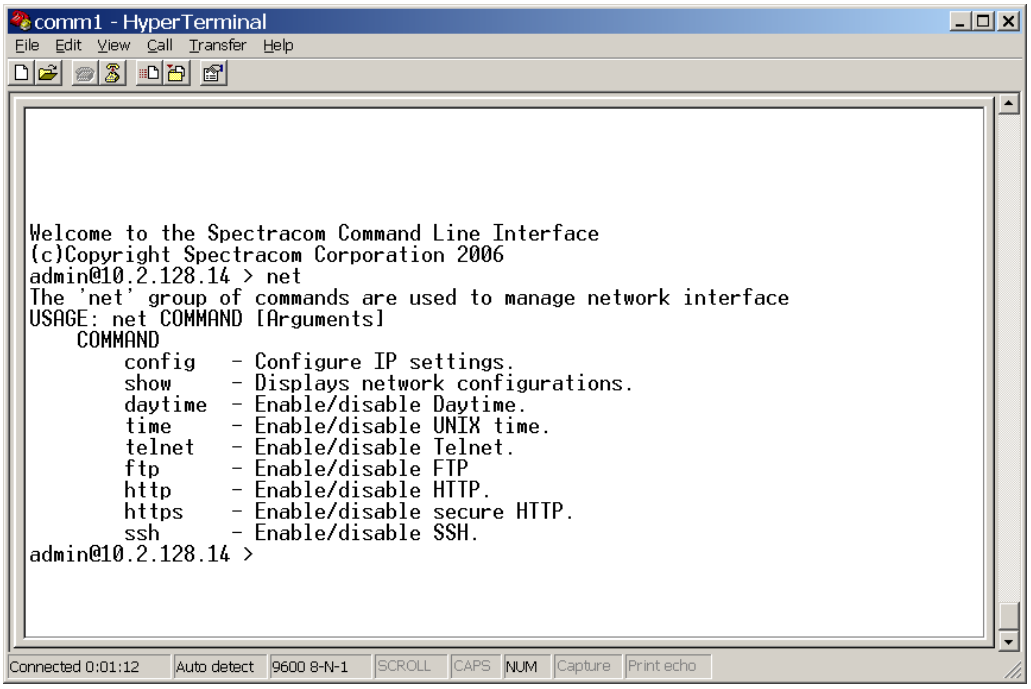

comm1 - HyperTerminal
File Edit View Call Transfer Help
Welcome to the Spectracom Command Line Interface
(c)Copyright Spectracom Corporation 2006
admin@10.2.128.14 > net
The 'net' group of commands are used to manage network interface
USAGE: net COMMAND [Arguments]
COMMAND
config - Configure IP settings.
show - Displays network configurations.
daytime - Enable/disable Daytime.
time - Enable/disable UNIX time.
telnet - Enable/disable Telnet.
ftp - Enable/disable FTP
http - Enable/disable HTTP.
https - Enable/disable secure HTTP.
ssh - Enable/disable SSH.
admin@10.2.128.14 >
Connected 0:01:12 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Figure 3-11: Net Commands

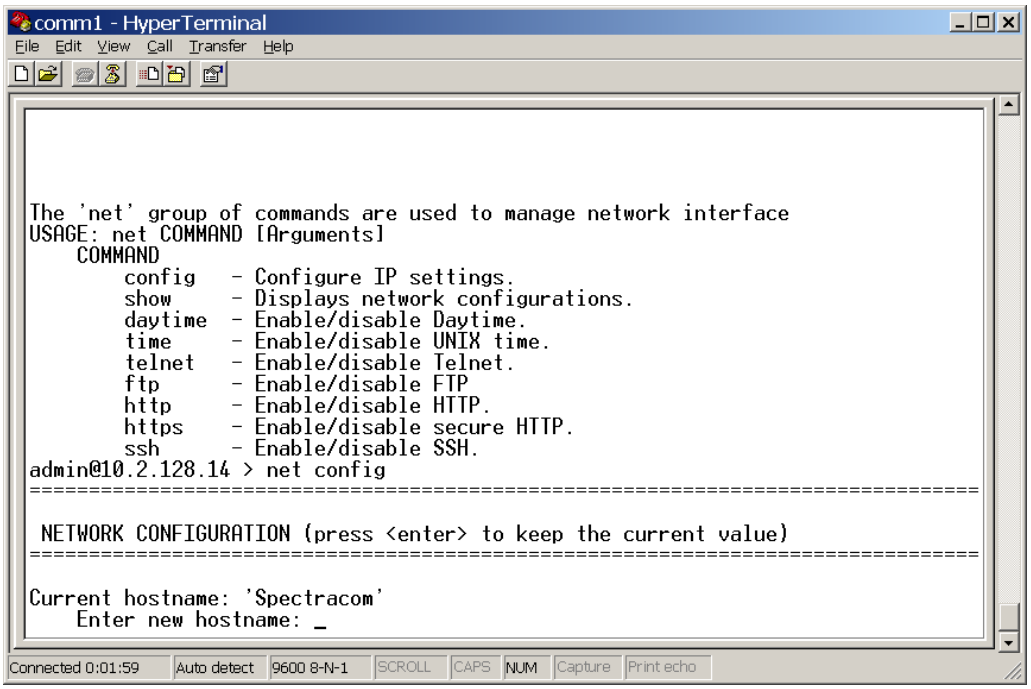

comm1 - HyperTerminal
File Edit View Call Transfer Help
The 'net' group of commands are used to manage network interface
USAGE: net COMMAND [Arguments]
COMMAND
config - Configure IP settings.
show - Displays network configurations.
daytime - Enable/disable Daytime.
time - Enable/disable UNIX time.
telnet - Enable/disable Telnet.
ftp - Enable/disable FTP
http - Enable/disable HTTP.
https - Enable/disable secure HTTP.
ssh - Enable/disable SSH.
admin@10.2.128.14 > net config
NETWORK CONFIGURATION (press <enter> to keep the current value)
Current hostname: 'Spectracom'
Enter new hostname: _
Connected 0:01:59 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Figure 3-12: Prompt for Initial Configuration Values in the CLI

During initial configuration, you will be prompted to enable or disable and enter, as necessary, various settings and addresses. The include the following:

Hostname: This is the network hostname that identifies the NetClock.

DNS Server: This is the IP address of the DNS server (if any).

DHCP Setting: This enables or disables DHCP. This must be set for IPv4 and IPv6. The NetClock always generates a static IPv6 address in addition to the dynamic IPv6 address(es).

Gateway: When the gateway IP is disabled on the product, the unit cannot be accessed from subnets outside the local subnet. When enabled, the IP address of the subnet's gateway must be specified. The default is disabled.

IP Address: This is the unique 32-bit static address assigned to the product. The default address is 10.10.200.1

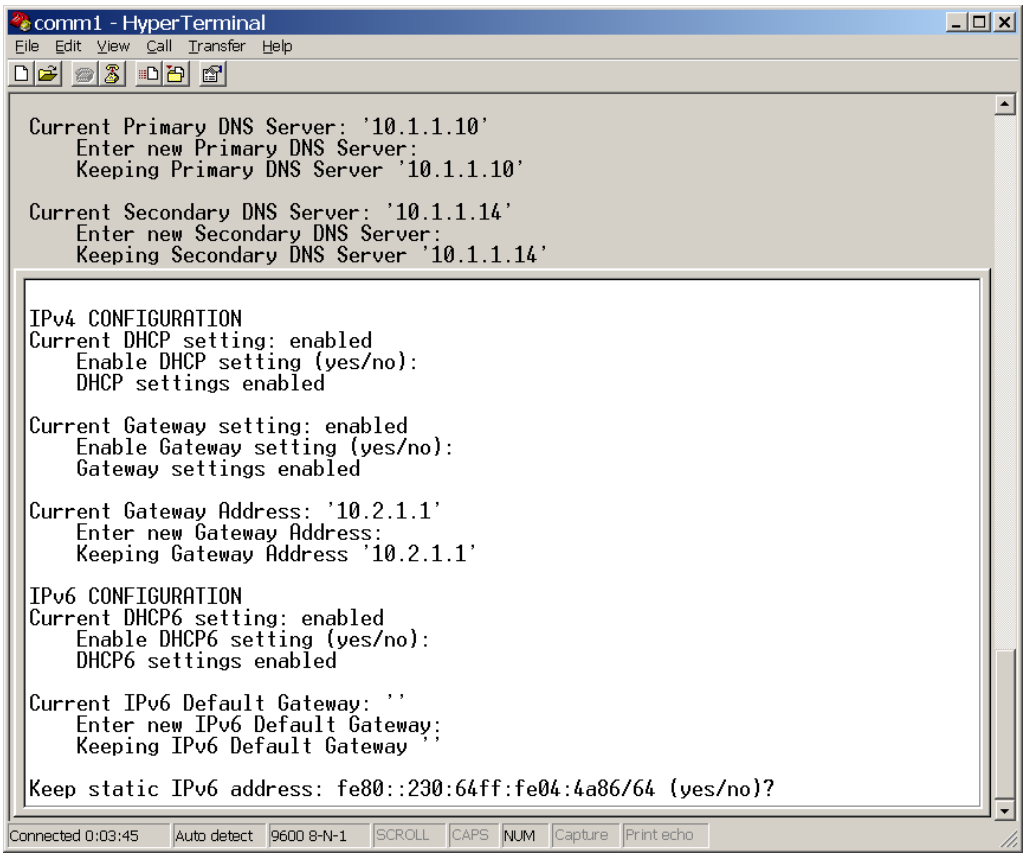

comm1 - HyperTerminal
File Edit View Call Transfer Help
Current Primary DNS Server: '10.1.1.10'
Enter new Primary DNS Server:
Keeping Primary DNS Server '10.1.1.10'
Current Secondary DNS Server: '10.1.1.14'
Enter new Secondary DNS Server:
Keeping Secondary DNS Server '10.1.1.14'
IPv4 CONFIGURATION
Current DHCP setting: enabled
Enable DHCP setting (yes/no):
DHCP settings enabled
Current Gateway setting: enabled
Enable Gateway setting (yes/no):
Gateway settings enabled
Current Gateway Address: '10.2.1.1'
Enter new Gateway Address:
Keeping Gateway Address '10.2.1.1'
IPv6 CONFIGURATION
Current DHCP6 setting: enabled
Enable DHCP6 setting (yes/no):
DHCP6 settings enabled
Current IPv6 Default Gateway: ''
Enter new IPv6 Default Gateway:
Keeping IPv6 Default Gateway ''
Keep static IPv6 address: fe80::230:64ff:fe04:4a86/64 (yes/no)?
Connected 0:03:45 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Figure 3-13: Initial Configuration using the CLI

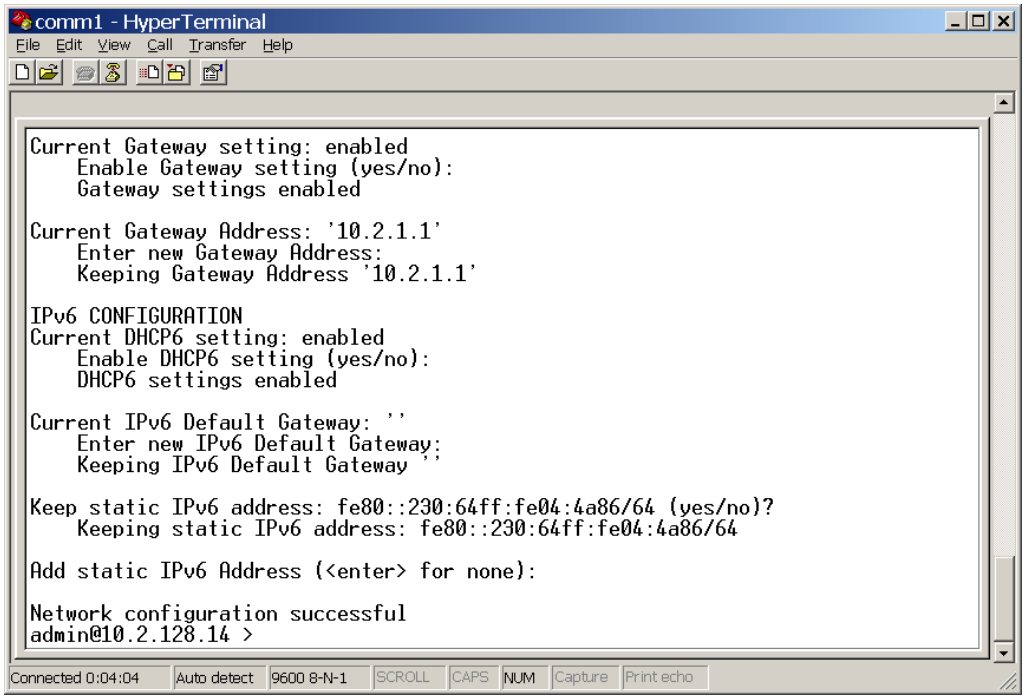


Figure 3-14: Successful Completion of Network Configuration

NOTE: All IPv4 addresses must be entered in “dotted quad” format. All IPv6 addresses must be entered in standard IPv6 address format.

NOTE: Setting the gateway to Disabled will cause the values in the Gateway Address field to be ignored.

NOTE: Changing the IP address of the NetClock to a different subnet will prompt the NetClock to start using the new IP address immediately. If you are connected to the CLI through a network instead of directly through the serial setup port, your session will end when the IP address is changed. Start a new session and use the new IP address to reconnect to the CLI.

3.2.3 Default and Recommended Configurations

The factory default configuration settings were chosen for ease of initial setup. Refer to the recommended settings listed here as applicable for your unit.

Configuration	Default	Recommended	Where Enabled
HTTP	Enabled	Disabled	Web User Interface or Command Line Interface
HTTPS	Enabled – Using customer-generated certificate and key or default Spectracom self-signed certificate and common public/private key SSH/SCP/SFTP enabled with unit unique 1024 bit keys		Web User Interface
SNMP	Disabled	Disabled or Enabled with: – SNMP v3 w/ encryption*	Web User Interface
NTP	Enabled – With no MD5 Values Entered	Enabled – Use MD5 authentication with user-defined keys	Web User Interface
Daytime Protocol	Disabled	Disabled	Web User Interface
Time Protocol	Disabled	Disabled	Web User Interface
Command Line Interface			
Console Port	Available – Unless dial-out modem connected (uses this port)	Available	Not Applicable
Telnet	Enabled	Disabled – Use SSH instead	Web User Interface
SSH	Enabled (default keys provided)	Enabled	Web User Interface
File Transfer			
FTP	Enabled	Disabled – Use SFTP or SCP	Web User Interface
SCP	Available	Available	Not Applicable
SFTP	Available	Available	Not Applicable

**We recommend secure clients use only SNMPv3 with authentication for secure installations.*

Table 3-2: Default and Recommended Configurations

3.3 Issuing the HALT Command before Removing Power

Once power is applied to the NetClock, it should not be removed unless the HALT command is issued to the unit. This prevents corruption of the NetClock file system.

CAUTION:

Once power is applied to the unit, DO NOT disconnect power unless the HALT command is first issued to the NetClock. To be absolutely certain that it is safe to remove power, wait 30 seconds after the HALT command is issued before removing power.

NOTE: The HALT command may be issued to the NetClock through the Web UI, through the CLI, or through SNMP. To restore your NetClock to Factory Defaults while halting/rebooting, refer to Section 3.4.11. To delete GPS position data, refer to Section 3.4.7.

3.3.1 Issuing the HALT Command through the Web UI

From the System Reboot/Halt page (Figure 3-15), click the Halt Now button. Wait 30 seconds after making the HALT request before removing power to the unit. (The system may also be rebooted from this screen.)

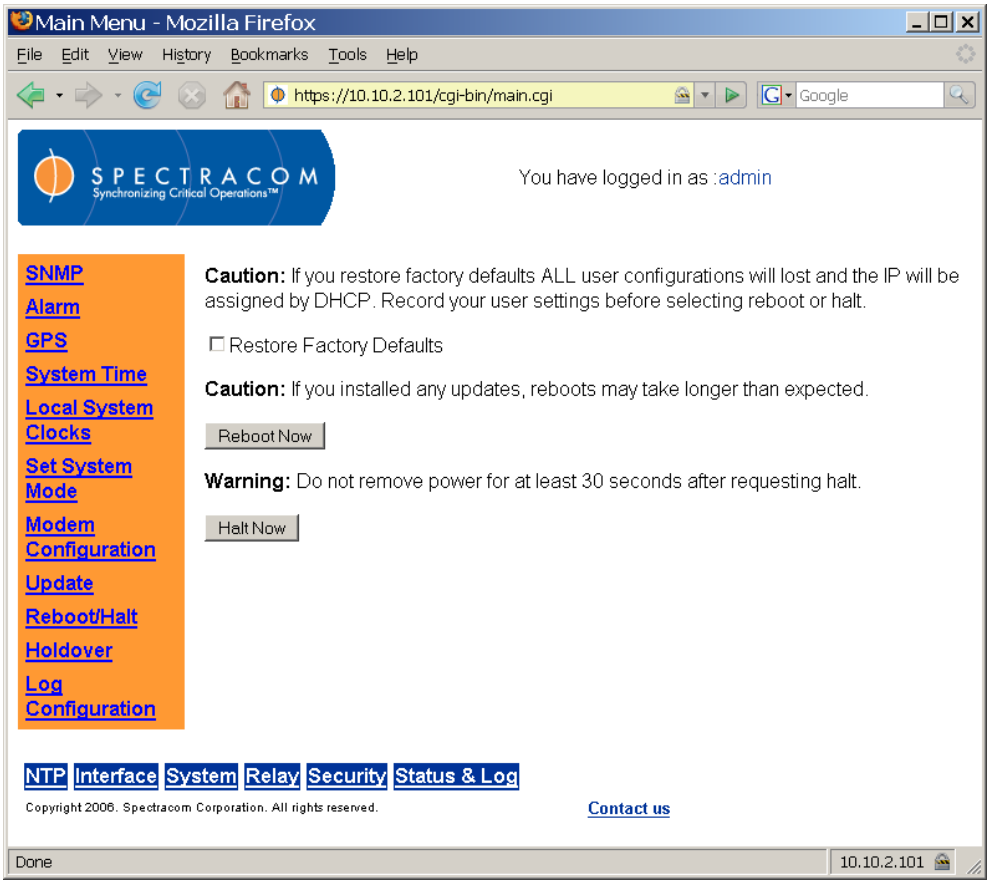

Main Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.10.2.101/cgi-bin/main.cgi
Google
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
SNMP
Alarm
GPS
System Time
Local System Clocks
Set System Mode
Modem Configuration
Update
Reboot/Halt
Holdover
Log Configuration
Caution: If you restore factory defaults ALL user configurations will lost and the IP will be assigned by DHCP. Record your user settings before selecting reboot or halt.
Restore Factory Defaults
Caution: If you installed any updates, reboots may take longer than expected.
Reboot Now
Warning: Do not remove power for at least 30 seconds after requesting halt.
Halt Now
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Done
10.10.2.101

Figure 3-15: System Reboot/Halt Screen (1 of 3)

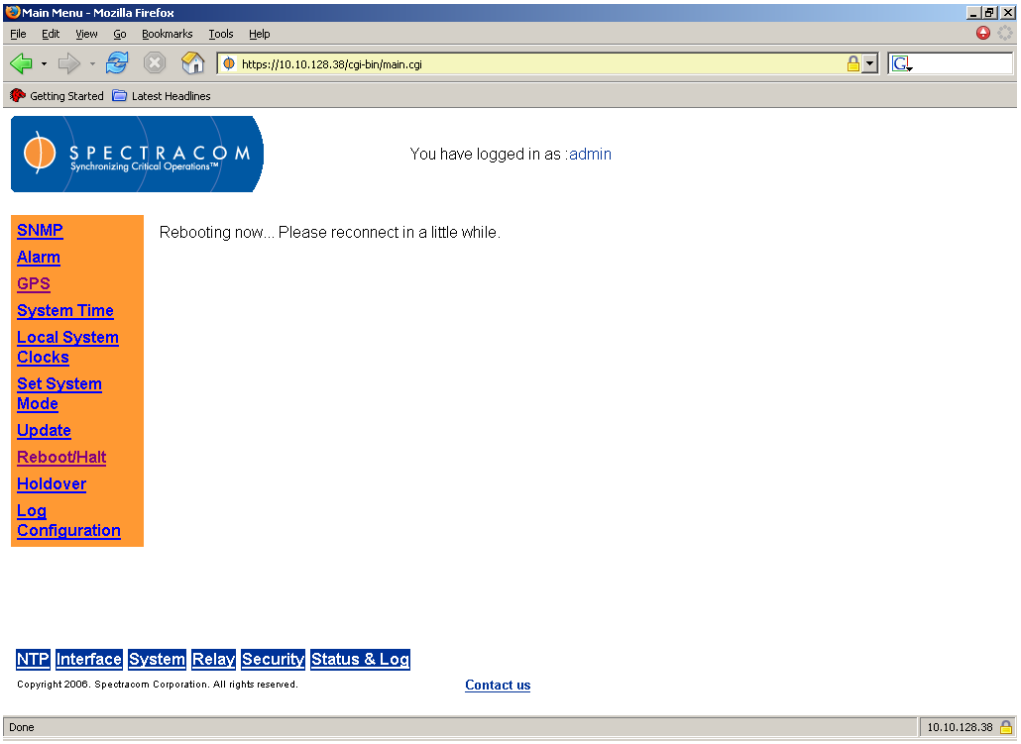


Figure 3-16: System Reboot/Halt Screen (2 of 3)

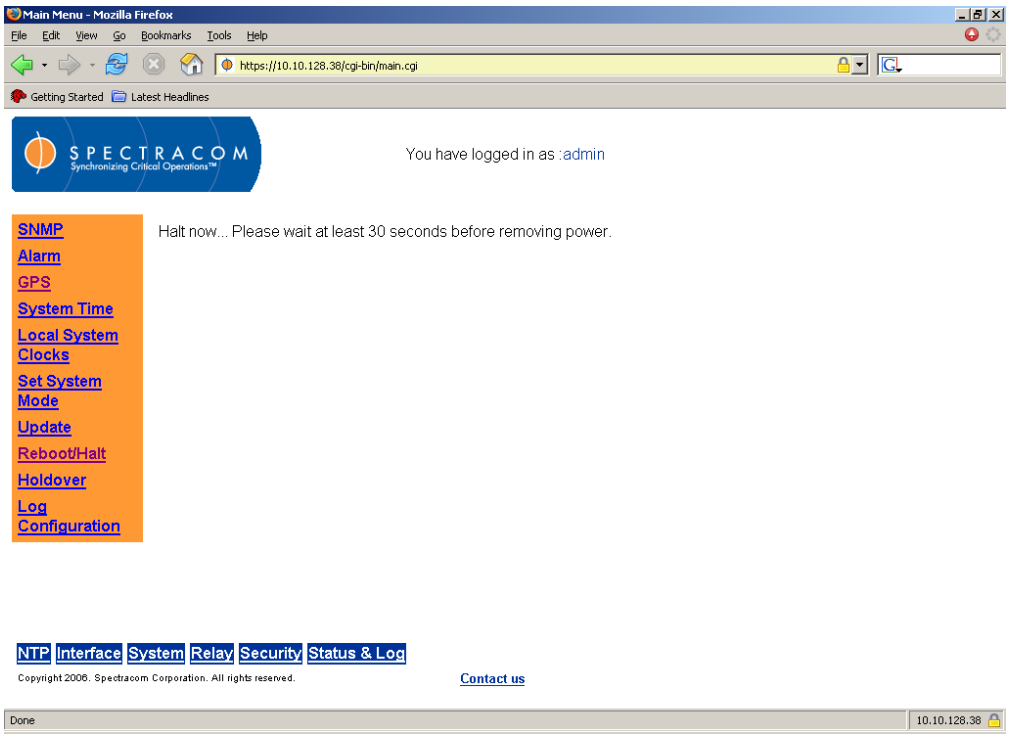


Figure 3-17: System Reboot/Halt Screen (3 of 3)

3.3.2 Issuing the HALT Command through the CLI

From the CLI (Figure 3-18), enter halt (Figure 3-19) Entering reboot will reboot the system (Figure 3-20).

NOTE: Wait 30 seconds after entering the HALT command before removing power.

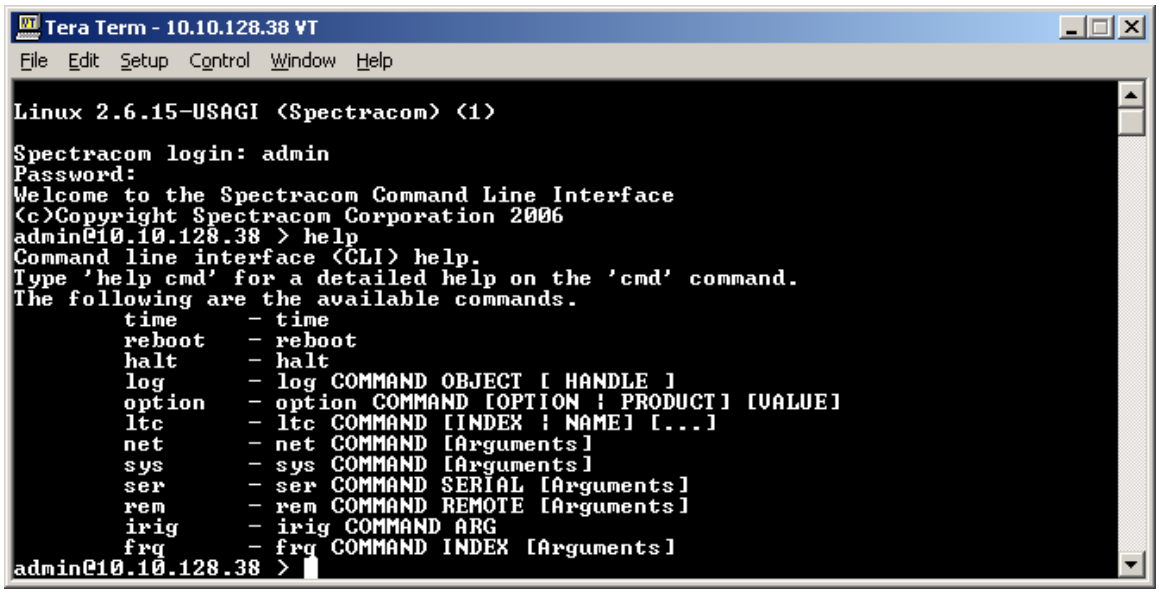

Tera Term - 10.10.128.38 VT
File Edit Setup Control Window Help
Linux 2.6.15-USAGI (Spectracom) (1)
Spectracom login: admin
Password:
Welcome to the Spectracom Command Line Interface
(c)Copyright Spectracom Corporation 2006
admin@10.10.128.38 > help
Command line interface (CLI) help.
Type 'help cmd' for a detailed help on the 'cmd' command.
The following are the available commands.
time - time
reboot - reboot
halt - halt
log - log COMMAND OBJECT [HANDLE]
option - option COMMAND [OPTION | PRODUCT] [VALUE]
ltc - ltc COMMAND [INDEX | NAME] [...]
net - net COMMAND [Arguments]
sys - sys COMMAND [Arguments]
ser - ser COMMAND SERIAL [Arguments]
rem - rem COMMAND REMOTE [Arguments]
irig - irig COMMAND ARG
frq - frq COMMAND INDEX [Arguments]
admin@10.10.128.38 >

Figure 3-18: Command Line Interface (CLI)

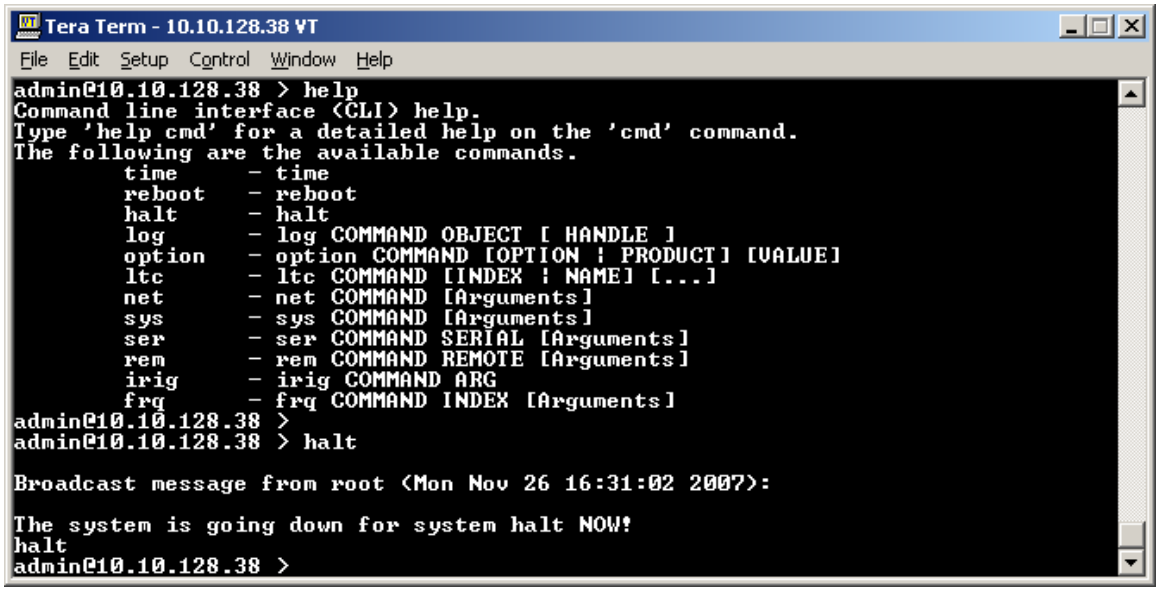

Tera Term - 10.10.128.38 VT
File Edit Setup Control Window Help
admin@10.10.128.38 > help
Command line interface (CLI) help.
Type 'help cmd' for a detailed help on the 'cmd' command.
The following are the available commands.
time - time
reboot - reboot
halt - halt
log - log COMMAND OBJECT [HANDLE]
option - option COMMAND [OPTION | PRODUCT] [VALUE]
ltc - ltc COMMAND [INDEX | NAME] [...]
net - net COMMAND [Arguments]
sys - sys COMMAND [Arguments]
ser - ser COMMAND SERIAL [Arguments]
rem - rem COMMAND REMOTE [Arguments]
irig - irig COMMAND ARG
frq - frq COMMAND INDEX [Arguments]
admin@10.10.128.38 >
admin@10.10.128.38 > halt
Broadcast message from root (Mon Nov 26 16:31:02 2007):
The system is going down for system halt NOW!
halt
admin@10.10.128.38 >

Figure 3-19: Halting the System from the CLI

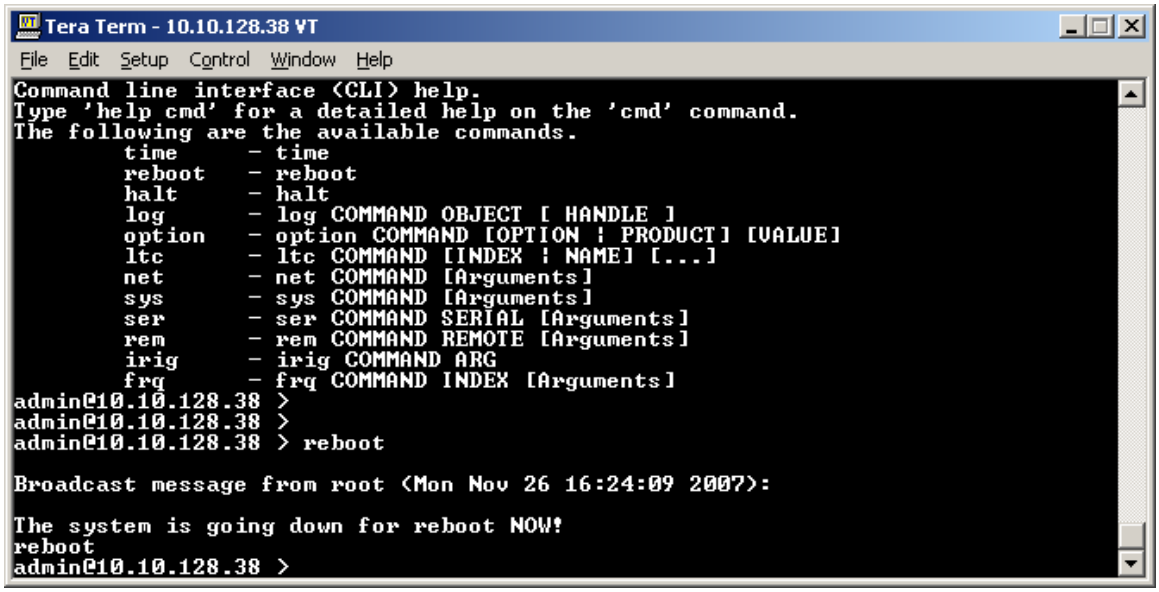

Tera Term - 10.10.128.38 VT
File Edit Setup Control Window Help
Command line interface (CLI) help.
Type 'help cmd' for a detailed help on the 'cmd' command.
The following are the available commands.
time - time
reboot - reboot
halt - halt
log - log COMMAND OBJECT [HANDLE]
option - option COMMAND [OPTION | PRODUCT] [VALUE]
ltc - ltc COMMAND [INDEX | NAME] [...]
net - net COMMAND [Arguments]
sys - sys COMMAND [Arguments]
ser - ser COMMAND SERIAL [Arguments]
rem - rem COMMAND REMOTE [Arguments]
irig - irig COMMAND ARG
frq - frq COMMAND INDEX [Arguments]
admin@10.10.128.38 >
admin@10.10.128.38 >
admin@10.10.128.38 > reboot
Broadcast message from root (Mon Nov 26 16:24:09 2007):
The system is going down for reboot NOW!
reboot
admin@10.10.128.38 >

Figure 3-20: Rebooting the System from the CLI

3.3.3 Issuing the HALT Command through SNMP

The Reboot MIB location options in the NetClock (Figure 3-21) are as follows:

- HALT to shutdown (***NOTE:*** Wait 30 seconds after shutting down before removing power)
- NO to do nothing
- YES to reboot the NetClock.

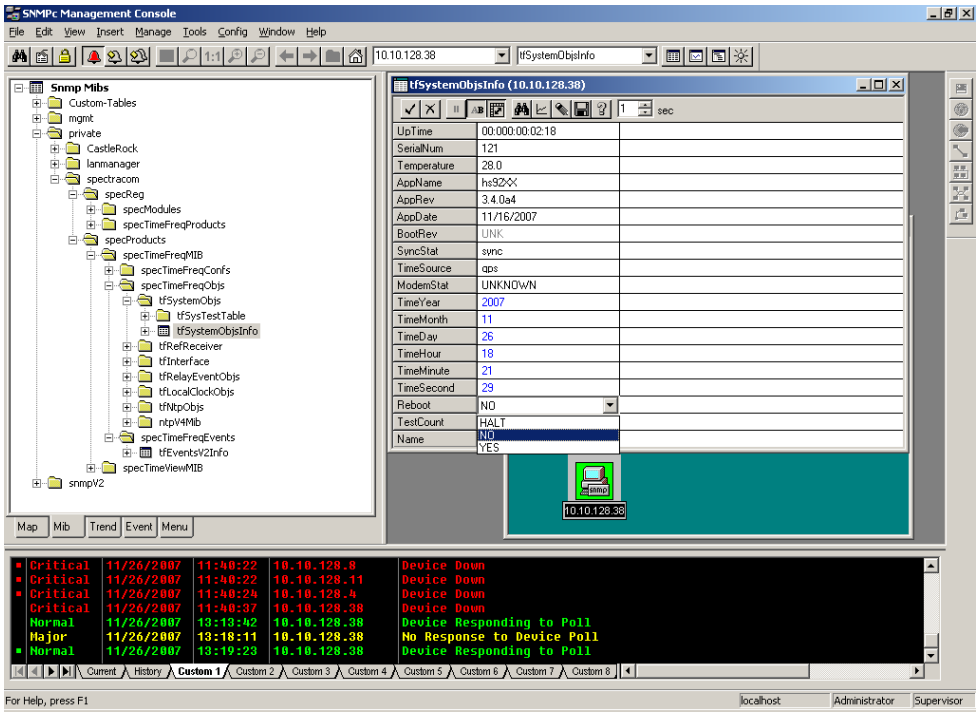


Figure 3-21: Reboot MIB Location Options (SNMP)

To reboot or halt the NetClock through SNMP, Spectracom provides a REBOOT MIB option. This is found in the tfSsytemObjsInfo table in the Spectracom Time and Frequency MIB under Spectracom Products specProduct, specTimeFreqMIB, in the specTimeFreqObjs under tfSystemObjs, in the table tfSystemObjsInfo. The REBOOT option (Figure 3-22) provides the choices of NO or YES for Reboot, and Halt to initiate a shut-down request.

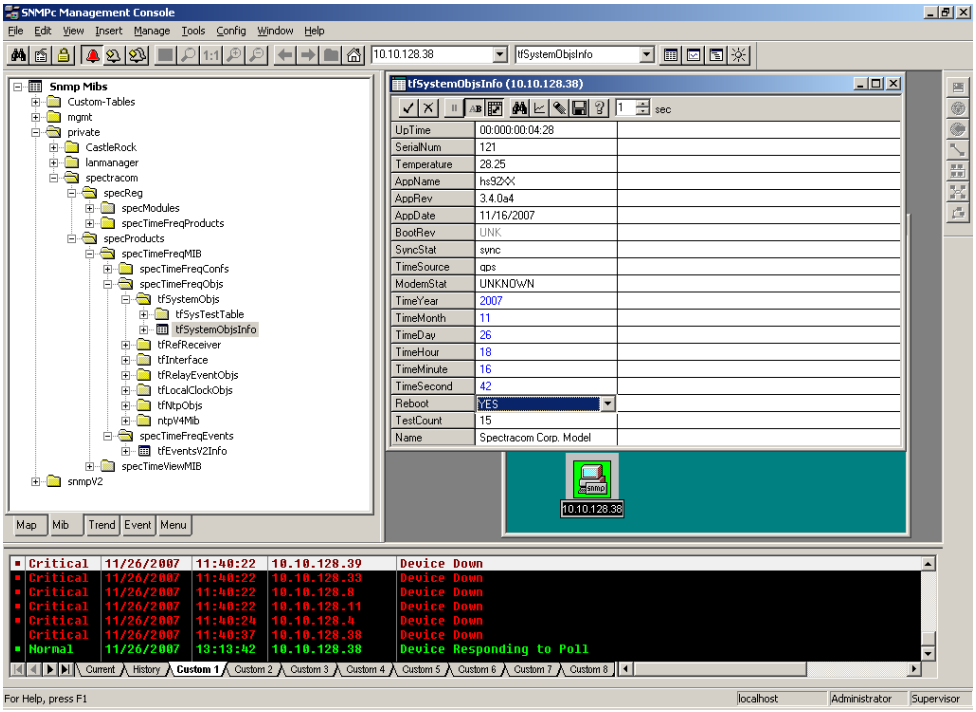


Figure 3-22: Rebooting the Unit through SNMP

To Reboot the unit, select YES and select the SET check box in the upper left corner of the SNMPc management console application. The Set operation reports success, but can with some SNMP managers return *Set Unsuccessful* due to a race condition in rebooting the unit and replying over SNMP. This is not an error.

To Halt the unit, select HALT and select the SET checkbox (Figure 3-23).

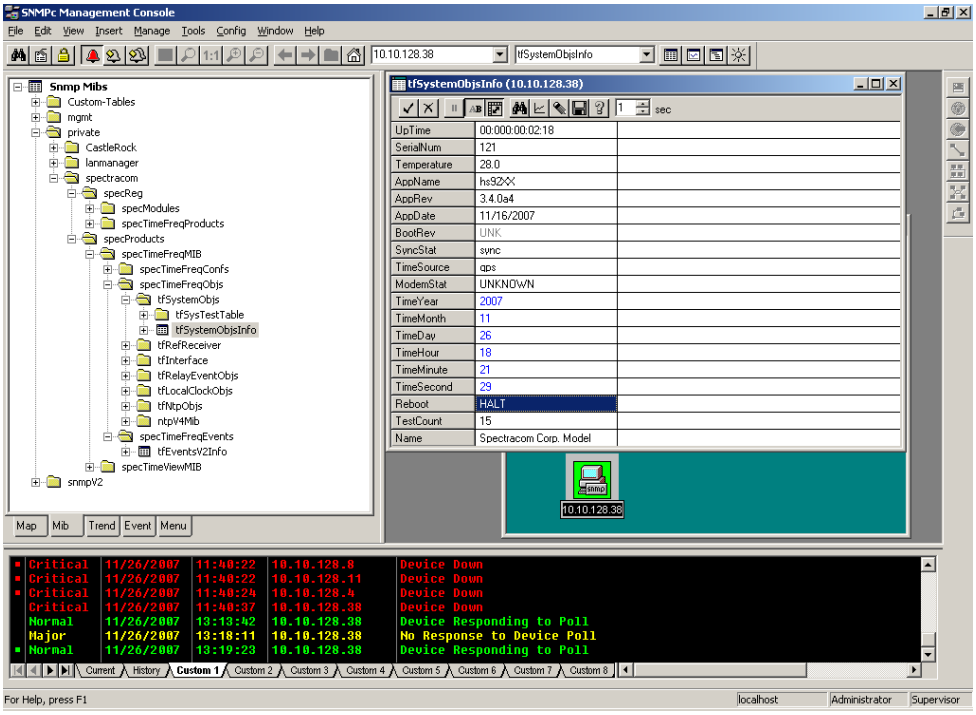


Figure 3-23: Halting the Unit through SNMP

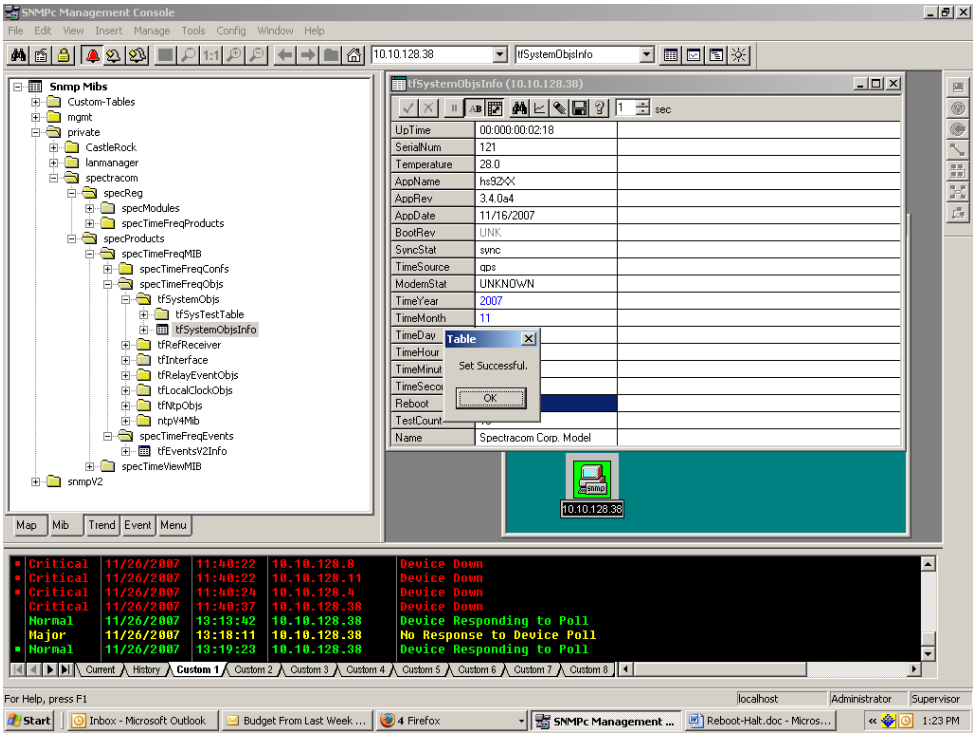


Figure 3-24: Successful Halt

The Set Successful Table box (Figure 3-24) will display to indicate that the Halt request to shut down the NetClock has been accepted. Wait 30 seconds before removing power.

3.4 Product Configuration using the WEB UI

With the NetClock connected to the network, you may configure it, change its operating settings, check its status, and generate reports from the Web UI as needed and desired. All Web UI screens are accessible through the menu at the bottom of the screen, which is displayed after a successful login. These screens, their functions, and example configurations (where applicable) are presented in this section.

NOTE: At any time during configuration in the Web UI, click "Submit" to save the settings or "Reset" to restore the settings to their previous state.

Figure 3-25: Web UI Primary Menu

3.4.1 Configuring NTP

The NTP menu groups the NetClock's NTP configuration and reporting functions (Figure 3-26). From this menu, the user may access the NTP General, References, Symmetrical Keys, Autokey, and Status screens.

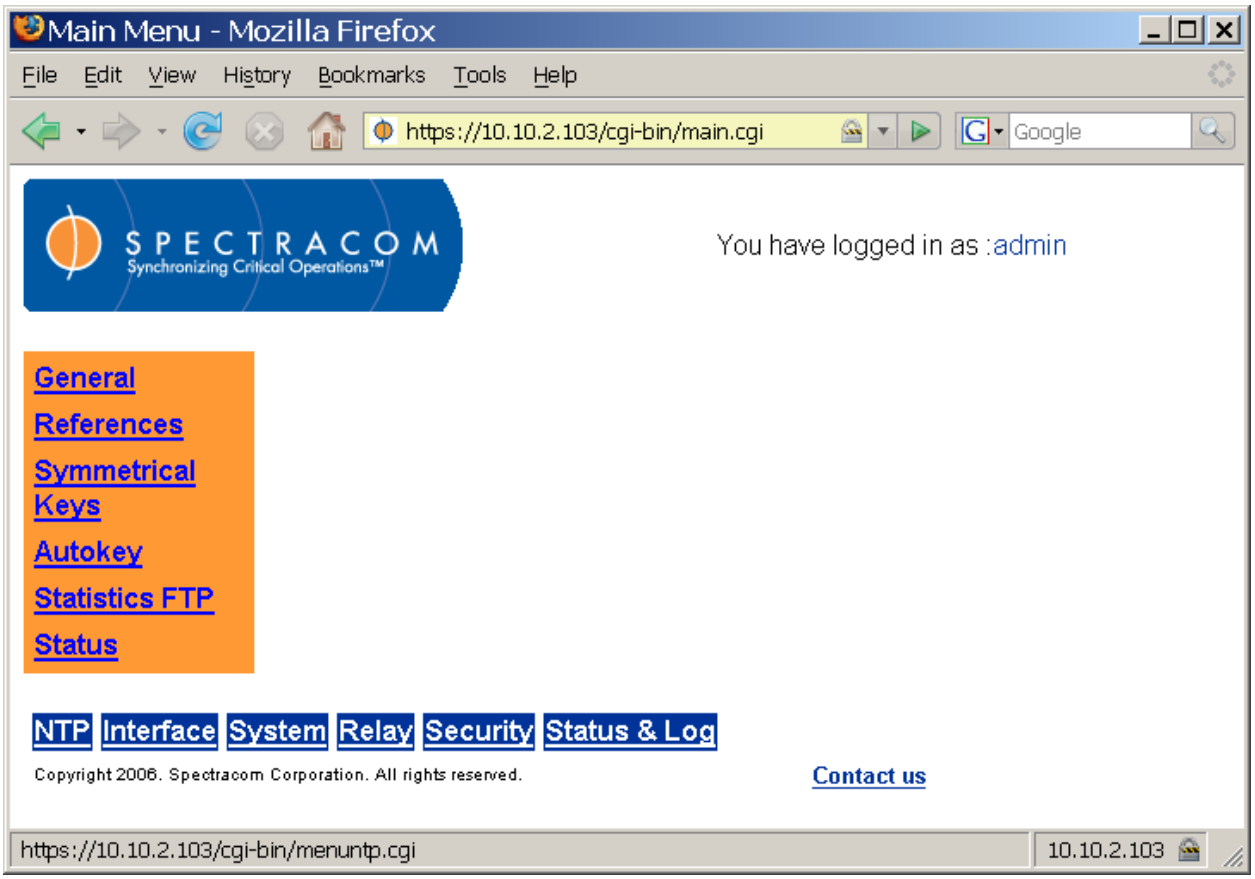


Figure 3-26: Web UI NTP Menu

Network Time Protocol (NTP) and Simple Network Time Protocol (SNTP) are client-server protocols for synchronizing time on IP networks. NTP provides greater accuracy and error checking than does SNTP. NTP and SNTP can be used to synchronize the time on any computer equipment compatible with the Network Time Protocol. This includes CISCO routers and switches, UNIX machines, and Windows machines with suitable clients. To synchronize a single workstation, several freeware or shareware NTP clients are available on the Internet. The software running on the PC determines whether NTP or SNTP is used.

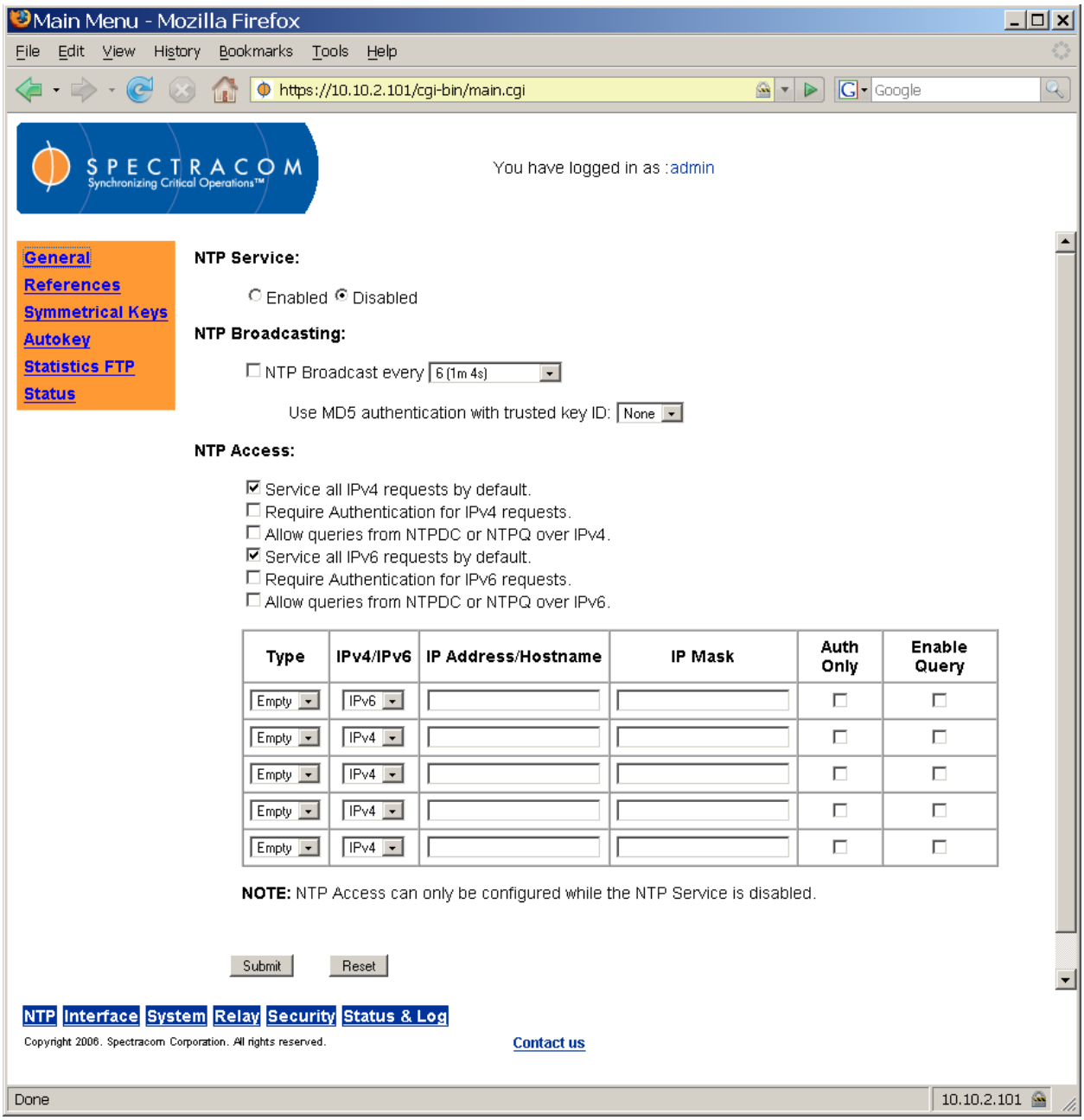


Figure 3-27: NTP General Screen

Refer to Figure 3-27. The user can enable or completely disable the NTP Service. When enabled, the NTP Service operates in unicast mode. In unicast mode the NTP Service

responds to NTP requests only. The NTP Service supports a broadcast mode in which it sends a NTP time packet to the network broadcast address. Check the box for NTP Broadcast to enable broadcast mode and select a rate at which to broadcast from the dropdown box. The NTP Broadcast mode is intended for 1 or a few servers and many clients. The NTP Broadcast rate should be selected based upon the network utilization and time drift in the clients. NTP broadcast can utilize MD5 authentication. Select a single MD5 key to use for broadcast from the pull-down menu. Use of MD5 authentication requires that MD5 symmetrical keys already be defined on the NTP Symmetrical Keys page. With the NTP service enabled and NTP broadcasting checked, the NetClock will operate in both modes.

When the NTP service is enabled, the NTP server will “listen” for NTP request messages from NTP clients on the network. When an NTP request packet is received, the NTP server will send an NTP response time packet to the requesting client. Under typical conditions, the Spectracom NTP server can service up to 4,000 NTP requests per second without MD5 authentication enabled (and a somewhat lower rate with MD5 authentication enabled).

When NTP broadcasting is selected, the NTP server will send unsolicited NTP time packets to the local broadcast address at a user-selected rate. The rates available are included in the dropdown menu. The NTP clients can use unicast, broadcast or a combination of both to discover and synchronize with the NTP server.

The NTP server supports authenticated NTP packets using an MD5 authenticator. This feature does not encrypt the time packets, but attaches an authenticator, which consists of a key identifier and an MD5 message digest, to the end of each packet. This can be used to guarantee that NTP packets came from a valid NTP client or server, and that they were not tampered with during transmission.

To use the MD5 authentication with trusted key ID, both the NTP client and the NetClock must contain the same key ID / key string pair and the client must be set to use one of these MD5 pairs. The key ID must be a number between 1 and 65532; the key string must be readable ASCII and between 1 and 16 characters long. Duplicate key IDs are not permitted. NTP requests received by the NTP server that do not contain an authenticator containing a valid Key ID and MD5 message digest pair will be responded to, but no authentication will be performed. NTP requests with valid authenticator result in a valid NTP response with its own valid authenticator using the same Key ID provided in the NTP request.

NTPDC and NTPQ are utilities for controlling NTP servers and gathering performance data from NTP servers. NetClock firmware 3.4.3 has facilities to allow these tools to gather performance data. Modification or control of a NetClock’s NTP service through NTPDC or NTPQ is not supported.

If you would like to allow any NTPDC or NTPQ client access over IPv4, enable “Allow Queries from NTPDC or NTPQ over IPv4.” If you would like this for IPv6 NTPDC or NTPQ, enable “Allow queries from NTPDC or NTPQ.”

Authentication is the use of some cryptographic technology to ensure that messages sent between computers are unaltered and emanate from a legitimate source.

NTP can use MD5 hashes along with trusted symmetric keys to ensure that messages come from authenticated sources. This does not encrypt NTP messages.

To require all requests for NTPDC or NTPQ to be authenticated over IPv4 or IPv6, enable "Allow Queries from NTPDC or NTPQ over IPv4" or "Allow queries from NTPDC or NTPQ over IPv6."

The NTP Access grid on the NTP General screen allows the user to enable or disable all IPv4 and IPv6 requests, as well as to allow or deny users or network segments. Clicking the "Auth Only" box on each line where a user or network segment is defined will prompt the NetClock to accept only authenticated requests (MD5 or Autokey) from this user or network segment.

You may also specify options on a per client basis. Instead of providing blanket access, you may specify which IP Addresses or hostnames have access, or restrict access for certain IP addresses or hostnames. To allow access, change the "Type" drop-down to "Allow," for restriction, to "Deny." Enter the appropriate hostname and IP Mask. If you wish for the additional security of authorized access, enable "Auth Only." To allow for queries, enable "Enable Query."

NOTE: Changes to the NTP configuration may only occur while the NTP service is disabled.

From the NTP References screen (Figure 3-28), the user may check the "Enable Stratum 0 Reference" box. This makes the 9383 a Stratum 1 reference. If this box is not checked, it means the NetClock is a Statum 2 (or higher) reference.

The grids on the NTP References screen allow the user to define, by IP address or hostname, the locations of other NTP servers to use as time references (instead of the configured NetClock's GPS reference) and the locations of other NTP servers to use as peers. Peers are NTP servers at the same stratum level that are used as an additional check on the NetClock's timing accuracy. This prevents it from moving to stratum levels farther away from Stratum 1 if the primary timing reference is lost. The maximum number of Peers allowed is 12. It is recommended to use one or more Peers when you desire to provide mutual backup. Each peer is normally configured to operate from one or more time sources including reference clocks or other higher stratum servers. If a peer looses all reference clocks or fails the other peers continue to provide time to other clocks on the network.

NTP servers can be configured as potential time references. The maximum number of NTP servers used as time references allowed is 12. For best results, more than 4 NTP time servers are recommended. As few as 1 NTP time server may be used, however, depending on your needs and network timing architecture. A specific NTP server can be configured as the preferred time reference by selecting the preferred checkbox. Only a single time reference can be selected as preferred and only when the Netclock is not in Stratum-1 mode using a Stratum-0 reference such as GPS, IRIG, Modem, or Serial Time Code Input.

For both NTP Peers and NTP Servers the Minimum and Maximum Poll rate for NTP packets can be configured. Both NTP Peers and NTP Servers support either manually configured Symmetric Key-ID/Key string pairs or the use of Auto-Key. However, these choices are mutually exclusive and must be identically configured on both the Netclock and the NTP Peer or NTP Server. If the Symmetric Key-ID/Key string pair method is selected the Key-ID must be first defined on the Symmetric Key page.

The entry for NTP Peer or NTP Server can be deleted by checking the Clear button and entering submit.

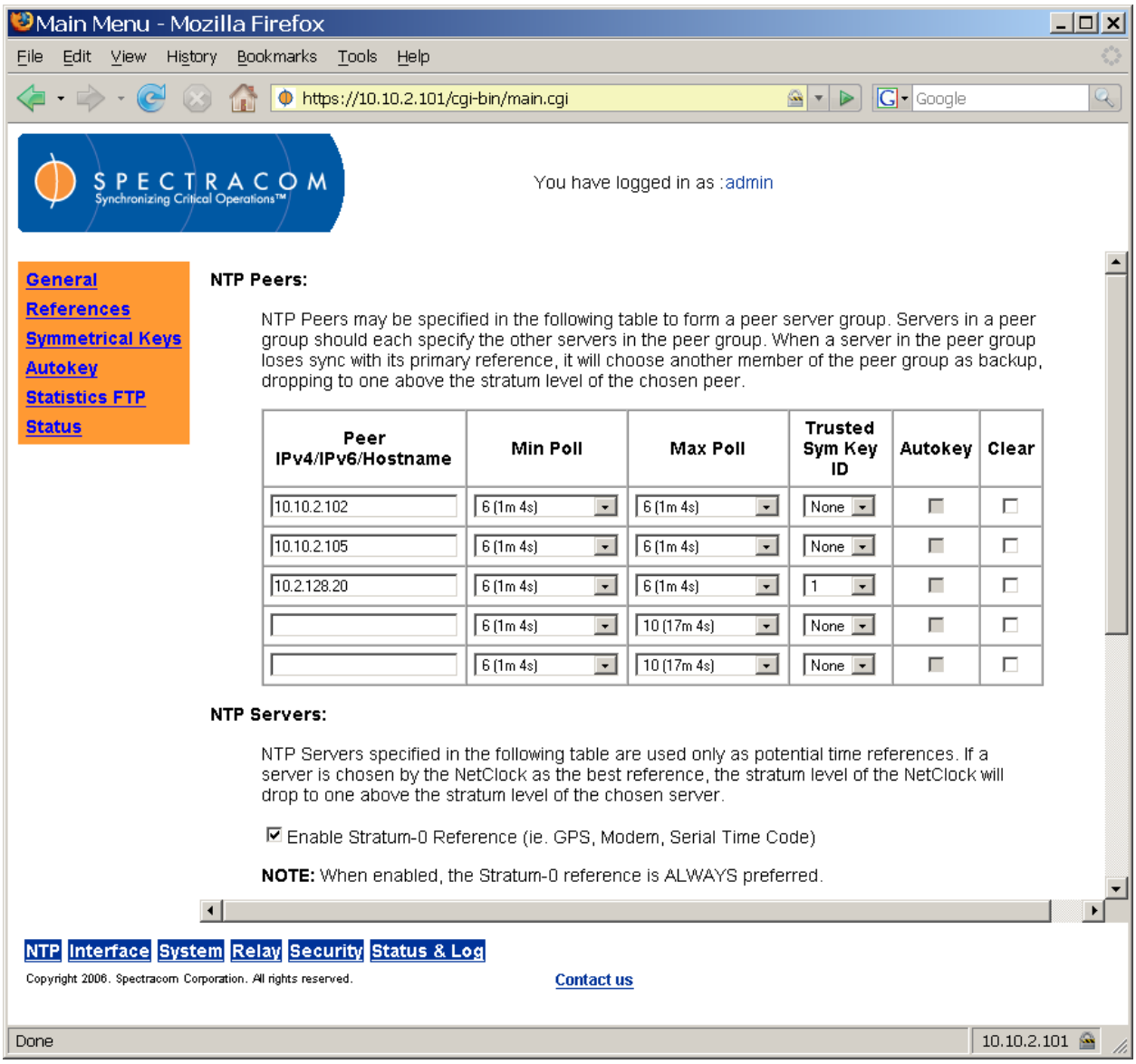

Main Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.10.2.101/cgi-bin/main.cgi
Google
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
General
References
Symmetrical Keys
Autokey
Statistics FTP
Status
NTP Peers:
NTP Peers may be specified in the following table to form a peer server group. Servers in a peer group should each specify the other servers in the peer group. When a server in the peer group loses sync with its primary reference, it will choose another member of the peer group as backup, dropping to one above the stratum level of the chosen peer.
Peer IPv4/IPv6/Hostname
Min Poll
Max Poll
Trusted Sym Key ID
Autokey
Clear
10.10.2.102
6 (1m 4s)
6 (1m 4s)
None
10.10.2.105
6 (1m 4s)
6 (1m 4s)
None
10.2.128.20
6 (1m 4s)
6 (1m 4s)
1
6 (1m 4s)
10 (17m 4s)
None
6 (1m 4s)
10 (17m 4s)
None
NTP Servers:
NTP Servers specified in the following table are used only as potential time references. If a server is chosen by the NetClock as the best reference, the stratum level of the NetClock will drop to one above the stratum level of the chosen server.
Enable Stratum-0 Reference (ie. GPS, Modem, Serial Time Code)
NOTE: When enabled, the Stratum-0 reference is ALWAYS preferred.
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Done
10.10.2.101

Figure 3-28: NTP References Screen (1 of 2)

NOTE: Check only ONE server as the preferred reference.

NOTE: You cannot use both a Trusted Symmetrical Key ID and Autokey. Autokey essentially automates the symmetrical key function and the two cannot be used together. If trusted keys have been defined (Figure 3-29), they will appear in the "Trusted Sym Key ID" dropdown menu.

NOTE: Checking the "Clear" box in the NTP References grids will immediately remove a defined server from the list.

The dropdown menus for "Min Poll" and "Max Poll" in the NTP References grids allow the user to choose, from within the available ranges, how often the NetClock will poll the defined servers

for timing information. Check with your network administrator for guidelines regarding network traffic and recommended polling intervals, if any.

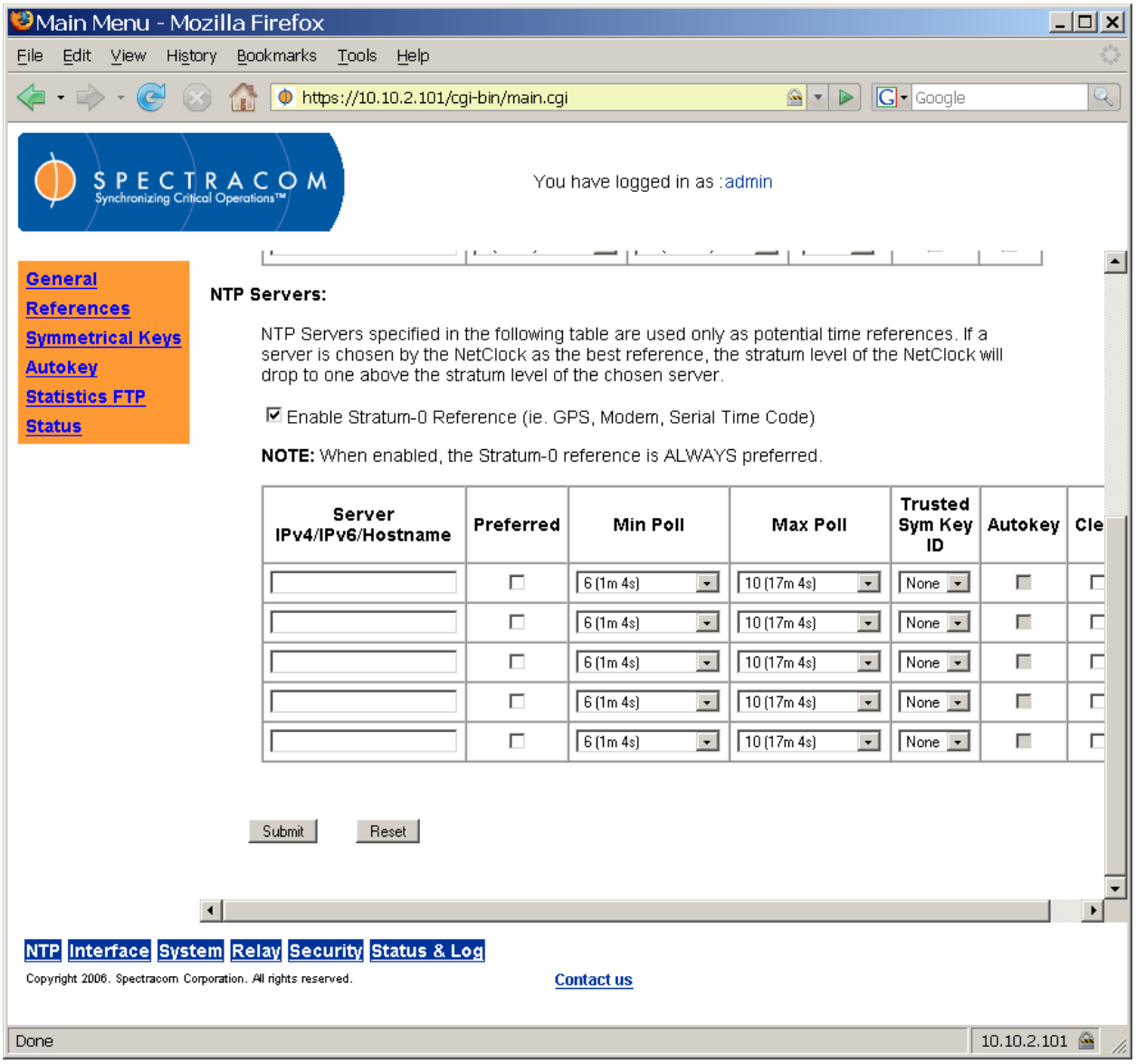

Main Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.10.2.101/cgi-bin/main.cgi
Google
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
General
References
Symmetrical Keys
Autokey
Statistics FTP
Status
NTP Servers:
NTP Servers specified in the following table are used only as potential time references. If a server is chosen by the NetClock as the best reference, the stratum level of the NetClock will drop to one above the stratum level of the chosen server.
Enable Stratum-0 Reference (ie. GPS, Modem, Serial Time Code)
NOTE: When enabled, the Stratum-0 reference is ALWAYS preferred.
Server IPv4/IPv6/Hostname
Preferred
Min Poll
Max Poll
Trusted Sym Key ID
Autokey
Cle
6 (1m 4s)
10 (17m 4s)
None
Submit
Reset
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Done
10.10.2.101

Figure 3-29: NTP References Screen (2 of 2)

From the Symmetrical Keys screen (Figure 3-30), the user may define the trusted symmetrical keys that must be entered on both the NetClock and any network client with which the NetClock is to communicate. The maximum number of Key-ID/Key String pairs is 15. Only those keys for which the "Trusted" box has been checked will appear in the dropdown menus on the NTP References screen (Figure 3-28).

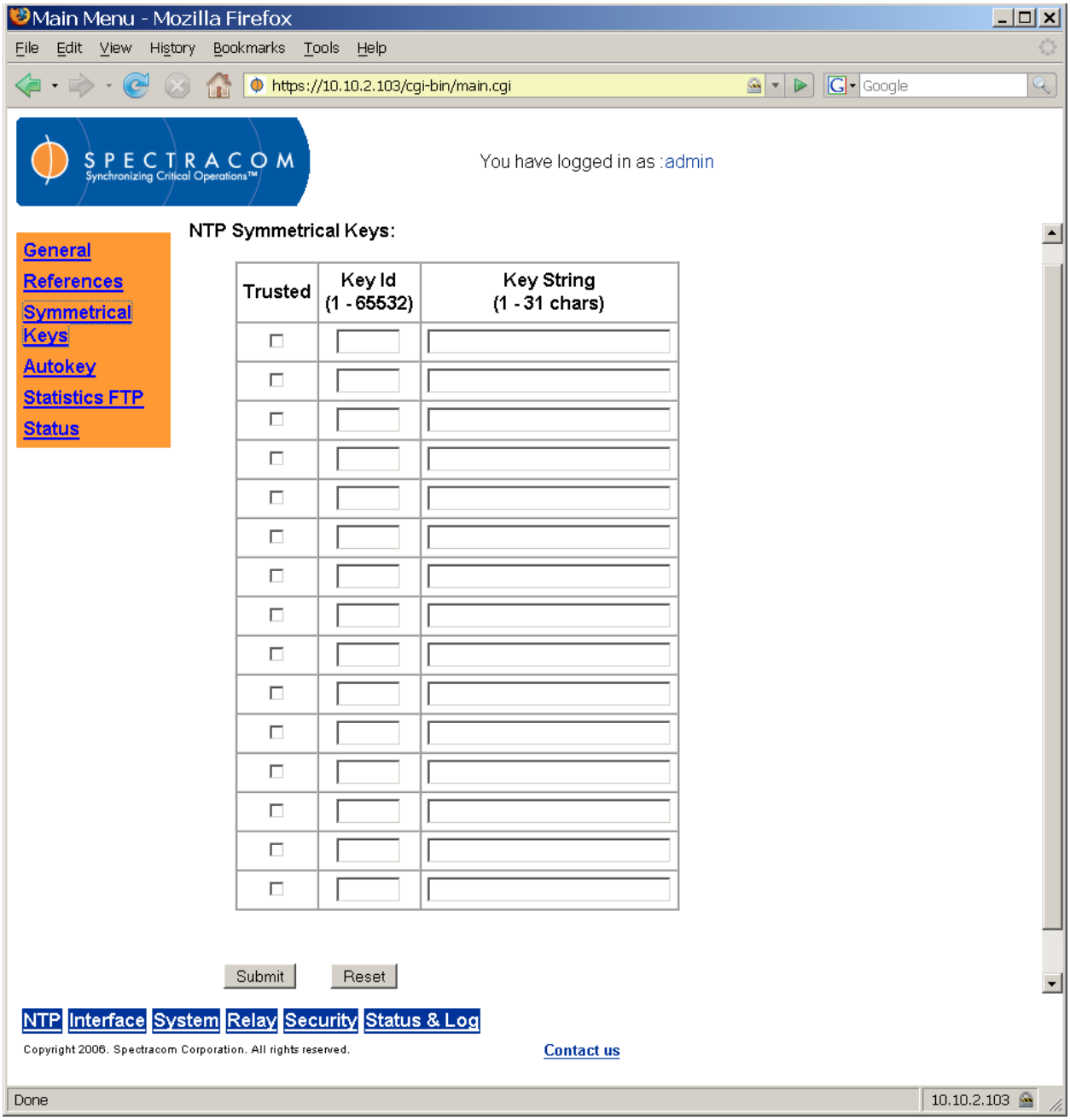


Figure 3-30: NTP Symmetrical Keys Screen

NOTE: It may be necessary to enter your username and password again in order to access the Symmetrical Keys screen.

Using Autokey essentially automates the trusted symmetrical key feature. From the Autokey screen (Figure 3-31), the user can click to enable or disable Autokey, enter a passphrase (readable ASCII, no spaces), and check “Generate Certificate” to generate a certificate in the text window at the bottom of the screen.

NOTE: Generate Certificate must always be clicked to generate the first certificate. If generating a new certificate after the first certificate, the menu will change to read “Regenerate Certificate.”

NOTE: Click the “Trusted” box on only ONE NetClock unit (the one that is closest to Stratum 0.)

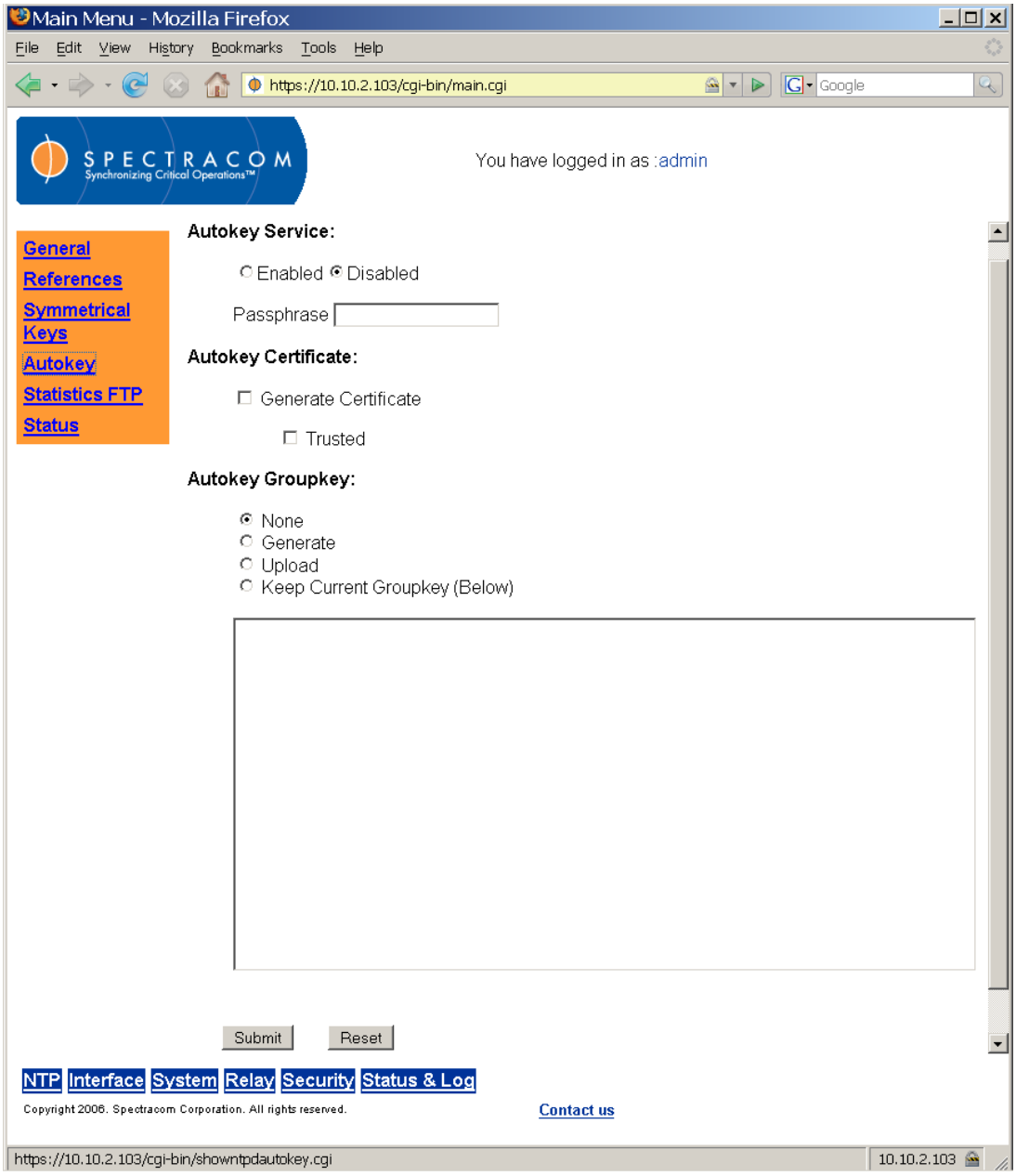


Figure 3-31: NTP Autokey Screen

NOTE: The Autokey feature can only be configured when NTP is disabled. If NTP is enabled, the fields in the Autokey screen cannot be accessed. To configure Autokey, disable NTP from the NTP General screen.

The user may also choose to use a Groupkey, which adds another level of authentication when using Autokey certificates. Click the “Generate” option under Autokey Groupkey to generate a certificate in the text window. Cut and paste this text into the text window on the other unit(s) and click the “Upload” option to upload it. Once an Autokey Groupkey has been generated the first time, the :”Keep Current Groupkey (Below)” option will be selected by default.

The Statistics FTP screen (Figure 3-32) allows the user to configure the locations to which the unit transmits NTP statistical data. Files are sent to the remote serve thirty minutes into every hour. Remote file names are appended with the UTC date stamp (YYYMMDD).

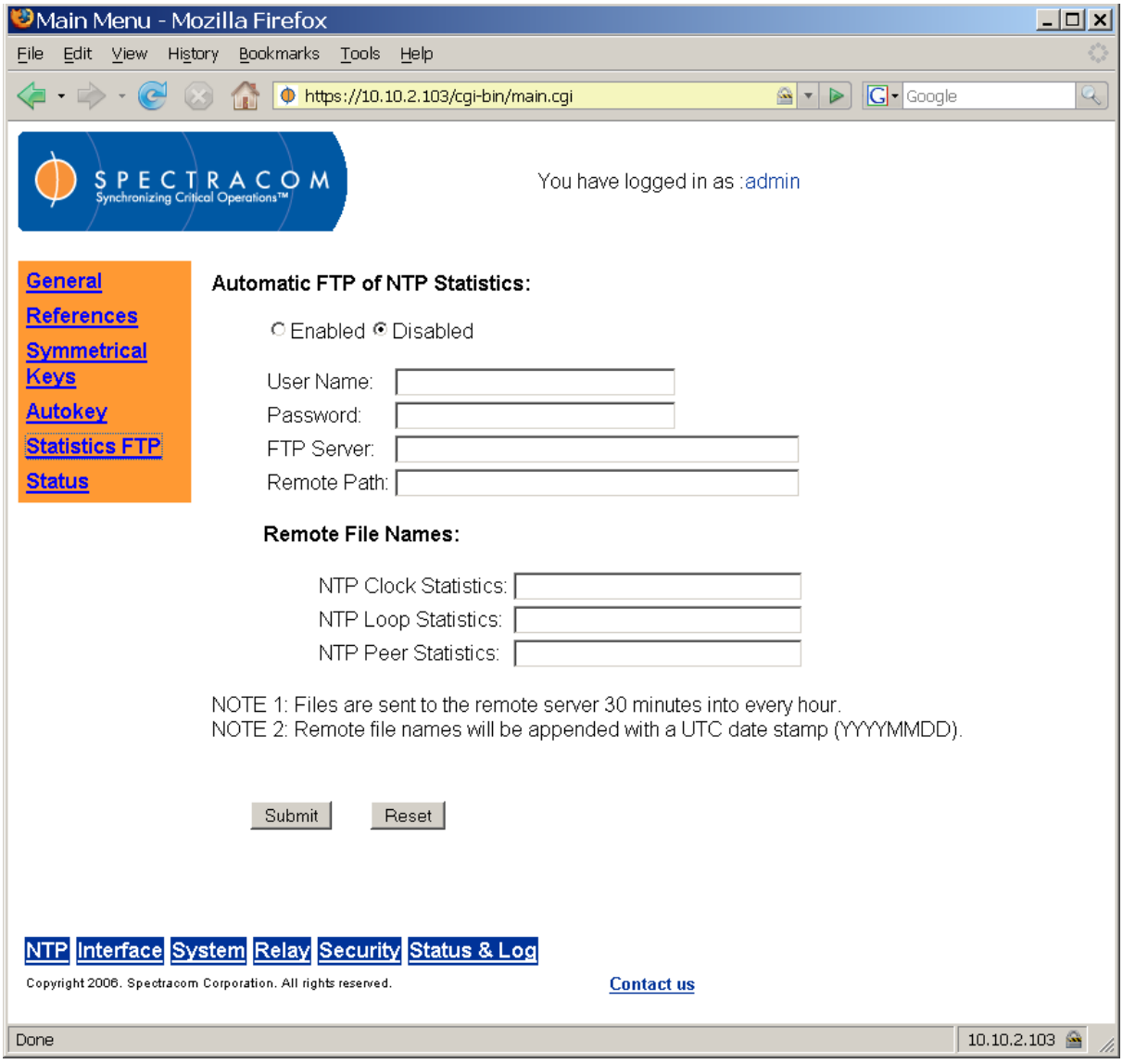


Figure 3-32: Statistics FTP Screen

The NTP Status screen (Figure 3-33) provides statistics and a graphical representation of various NTP statistics relevant to the NetClock's function. This includes whether the NetClock is time synchronized, its stratum level, the location of its selected reference, its delay, offset, and jitter, and statuses for defined timing references on the network.

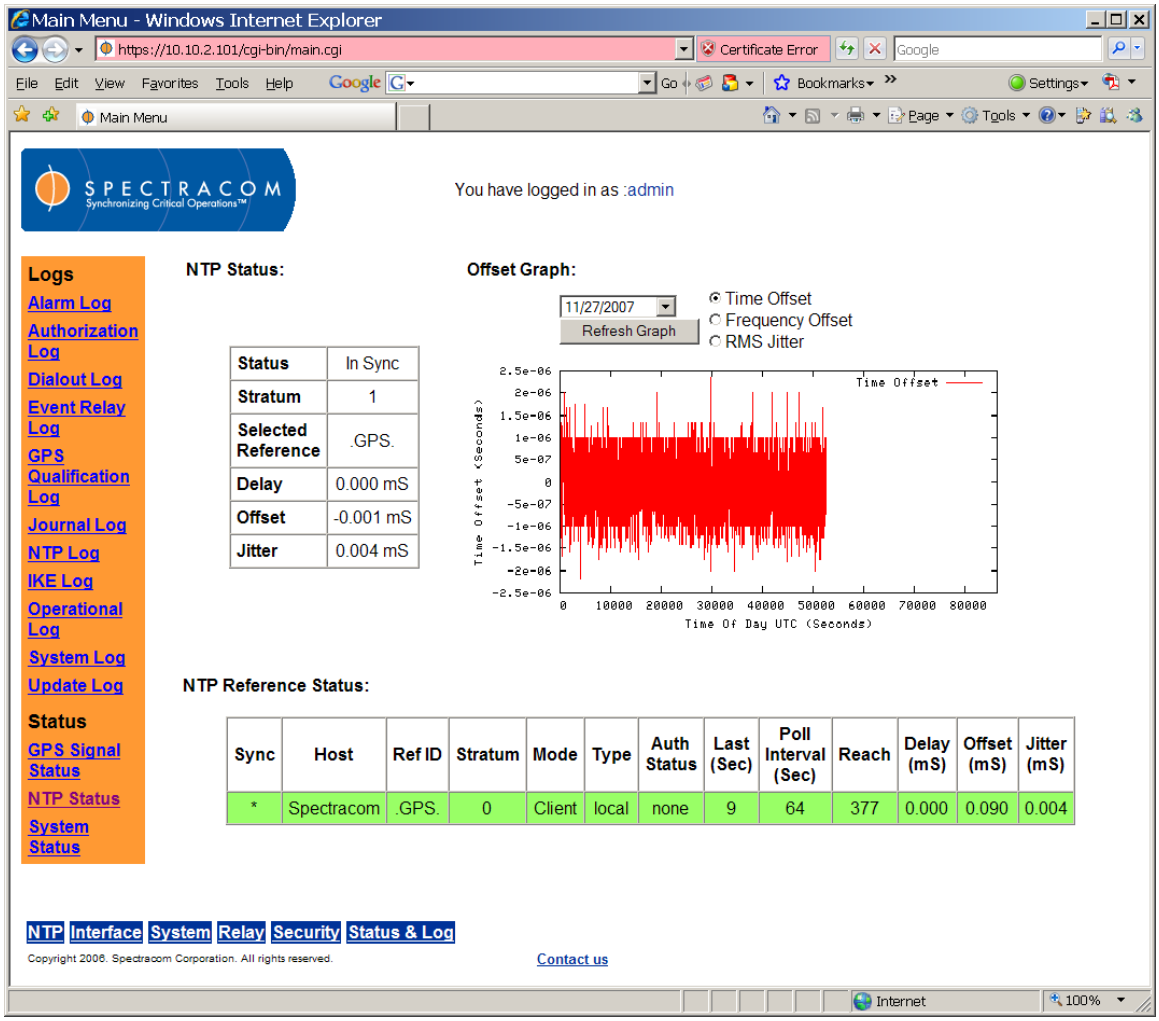


Figure 3-33: NTP Status Screen

NOTE: The NTP Reference Status lines bear different colors for different codes. Red is a reject (the peer is discarded as unreachable). Yellow is an outlyer (the peer is discarded by the clustering algorithm). Green is a candidate (the peer is a survivor and a candidate for the combining) or a syspeer/ppspeer (the peer has been declared the system peer and lends its variables to the system variables).

3.4.2 NTP Support

Spectracom cannot provide technical assistance for configuring and installing NTP on Unix-based applications. Please refer to **www.ntp.org/** for NTP information and FAQs. Another good source for support is the Internet newsgroup at **news://comp.protocols.time.ntp/**.

Spectracom can provide support for the Windows NT, Windows 2000, and Windows XP time synchronization. Refer to the Spectracom Web page, **www.spectracomcorp.com**, for more information, or contact Spectracom Technical Support by phone at **US +1.585.321.5800**.

3.4.3 Configuring the Interface

The Interface menu (Figure 3-34) groups the NetClock's Interface configuration functions. From this menu, the user may access the Interface Serial Port, Remote Port, IRIG, Display, and Frequency Output screens. The user may also use this menu to set the interface configuration to the factory default settings.

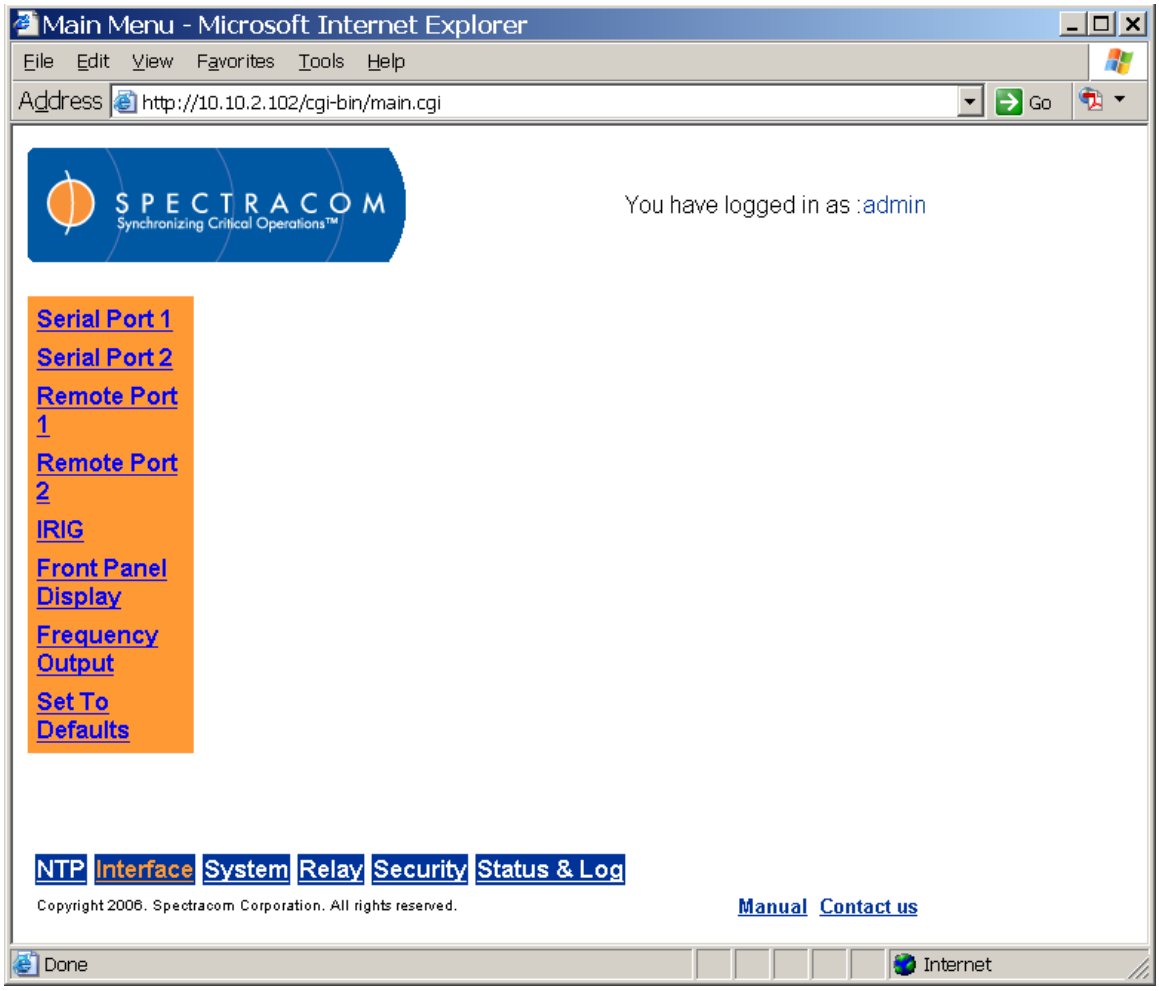


Figure 3-34: Interface Menu

The NetClock has two serial ports (RS-232 ports) and two remote output ports (RS-485 ports) that support independent output of date/time stamps from the NetClock. From the respective screens for the serial and remote ports (Figure 3-35 and Figure 3-36), the user may define the baud rate and the Data Format for each port. The system clock may also be selected if a local clock (set for a local time zone) has been defined. Serial ports include the "Request Char" feature, which allows the user to choose between multicast (broadcasting once per second on the second through the port) and a user-defined character. When the character of the user's

choice is entered, the NetClock will broadcast through the port only when that character is received by the unit.

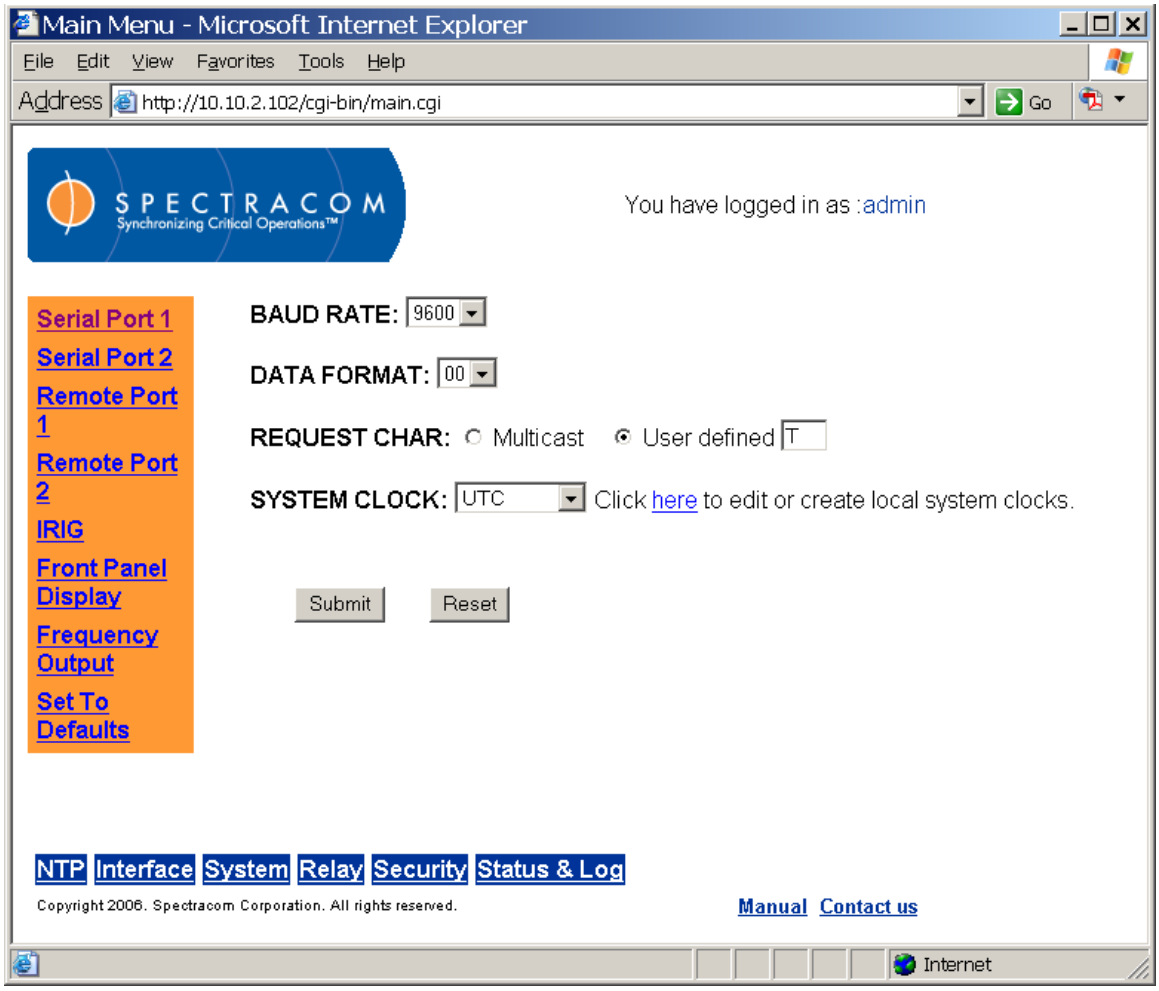


Figure 3-35: Interface Serial Port 1 Screen

The baud rate is the speed at which the port will output values. This speed must be selected from the dropdown box. The default is 9600 baud.

The Data Fomat is the format in which the date and time stamps are sent from the NetClock. Several Data Formats are supported. The default is Format 0.

NOTE: When connecting the remote output to a 9388 unit, the **DATA FORMAT** must be set to match the NetClock's remote output data format. If these values do not match, the 9388 cannot synchronize. By factory default, NetClock (non-9388 time server units) output Data Format 00, while the 9388 is factory configured to receive Data Format 02. Spectracom recommends using Data Format 02, meaning the Data Format value in the NetClock must be changed from the factory default to match the factory default of the 9388.

NOTE: Data Format 2 is always a Coordinated Universal Time (UTC) output. It cannot have a Time Zone Offset or the Daylight Saving Time (DST) rule enabled. Conversion to local lime is accomplished by the device receiving the data. An error will be generated if a Time Zone Offset or DST rule is applied to Data Format 2. NTP never outputs local time.

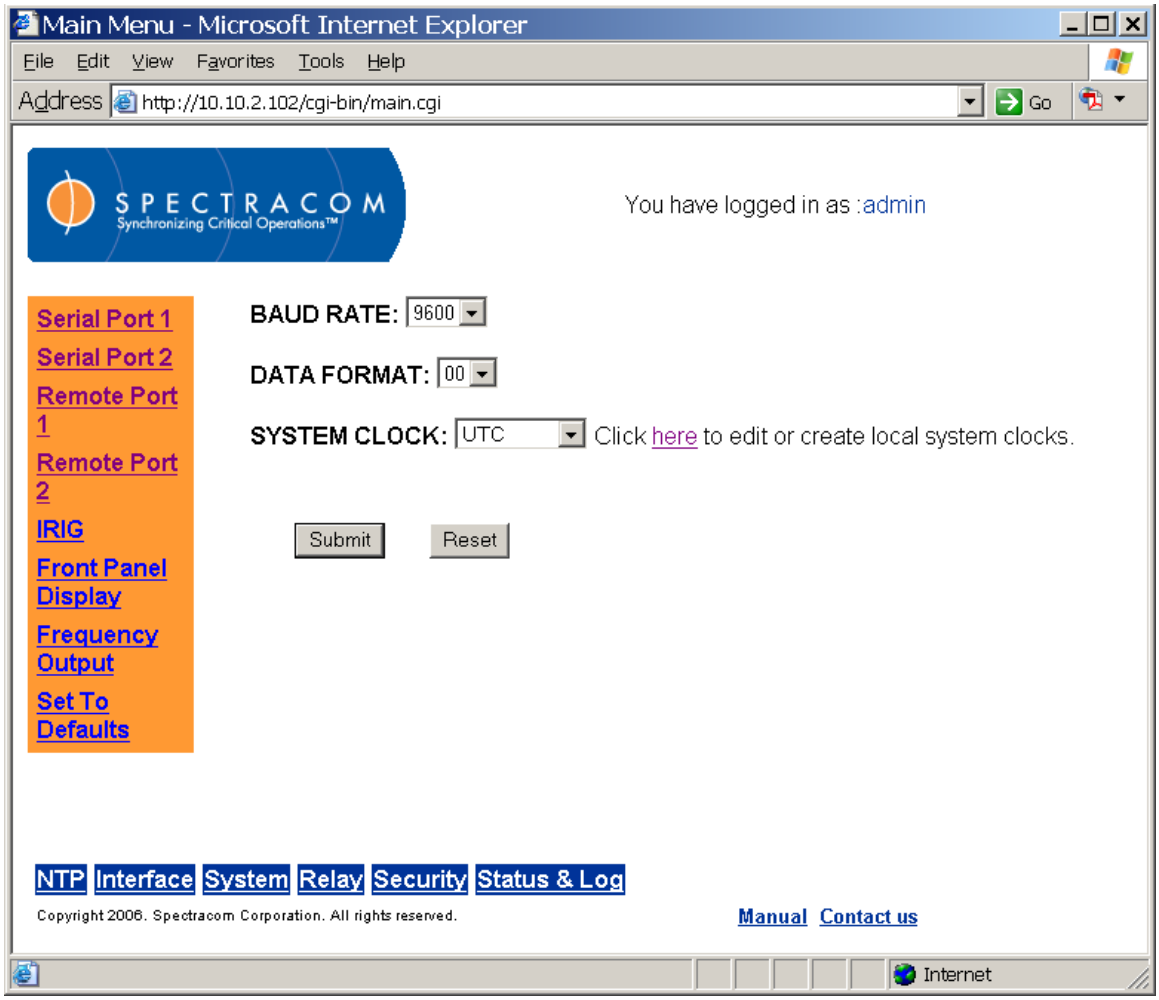


Figure 3-36: Interface Remote Port 2 Screen

Clicking the link to create and edit local systems clocks will display the Local System Clock screen. Refer to the System configuration screens in this manual for information on setting and editing local system clocks.

From the Interface IRIG screen, the user may configure the IRIG format, amplitude control, and signature. IRIG is an acronym for Inter-Range Instrumentation Group. In the late 1950s, this group created a series of time code standards suitable for use with recording oscillographs, magnetic tape, and real time transmission.

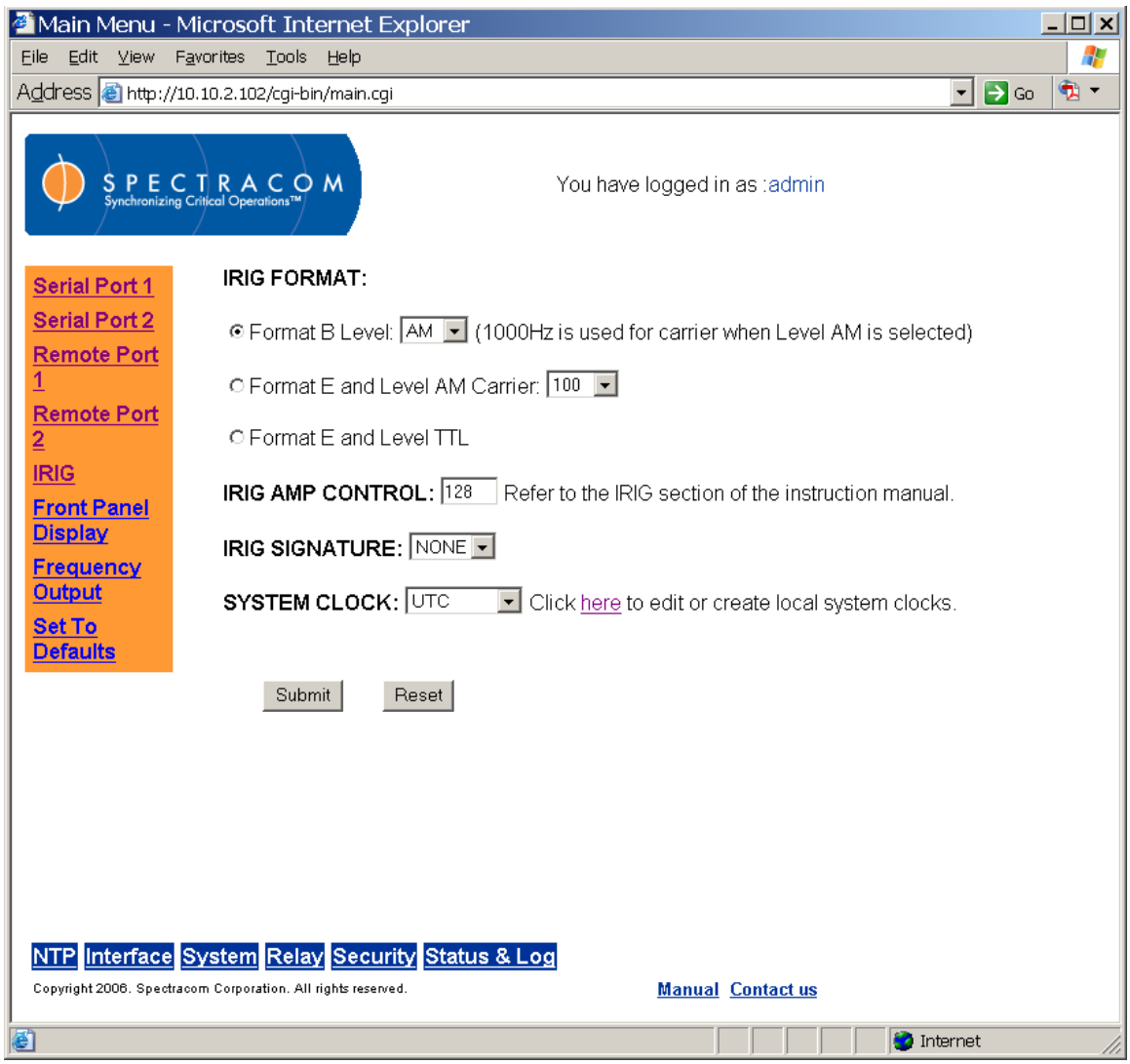

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Serial Port 1
Serial Port 2
Remote Port 1
Remote Port 2
IRIG
Front Panel Display
Frequency Output
Set To Defaults
IRIG FORMAT:
Format B Level: AM (1000Hz is used for carrier when Level AM is selected)
Format E and Level AM Carrier: 100
Format E and Level TTL
IRIG AMP CONTROL: 128 Refer to the IRIG section of the instruction manual.
IRIG SIGNATURE: NONE
SYSTEM CLOCK: UTC Click here to edit or create local system clocks.
Submit
Reset
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Internet

Figure 3-37: Interface IRIG Screen

Each IRIG code specifies a carrier frequency that is modulated to encode date and time, as well as control bits to time-stamp events. Initially, IRIG applications were primarily military and government associated. Today, IRIG is commonly used to synchronize voice loggers, recall recorders, and sequential event loggers found in emergency dispatch centers and power utilities.

Format	Encoding	Bit rate	Modulation	Time Frame Interval	Carrier	Coded Expressions
B	B120	100 pps	AM	1 sec	1 kHz	BCD_{TOY}, CF, SBS
B	B000	100 pps	PW	1 sec	N/A	BCD_{TOY}, CF, SBS
E	E111	10 pps	AM	10 sec	100 Hz	BCD_{TOY}, CF
E	E121	10 pps	AM	10 sec	1 kHz	BCD_{TOY}, CF
E	E001	10 pps	PW	10 sec	N/A	BCD_{TOY}, CF

NOTE: The Spectracom IRIG formats use the control functions for BCD year information and a Time Sync Status bit and in format E the control functions are used for straight binary seconds (SBS). Refer to individual IRIG Time Code description figures and text. IRIG Standard 200-98 format B had 27 control bits and format E had 45 bits for control functions. These control bits could be used for any use and there was no defined function. Spectracom used the control function element at index count 55 as the TIME SYNC STATUS and the sub-frame after position identifiers P6 and P7 as the year info and for format E the sub-frame after P8 and P9 for the straight binary seconds (SBS). The position of the BCD year information does not conform to the newer IRIG Standard 200-04. IRIG Standard 200-04 incorporated the year information after P5 and reduced the allocated control bits to 18 for format B and 36 for format E.

NOTE: DCLS is *DC Level Shifted* output, pulse width modulated with a position identifier having a positive pulse width equal to 0.8 of the reciprocal of the bit rate, a binary one (1) having a positive pulse width equal to 0.5 of the reciprocal of the bit rate and a binary zero (0) having a positive pulse width equal to 0.2 of the reciprocal of the bite rate.

The NetClock can provide an IRIG B or IRIG E code in amplitude modulated (AM) or pulse width coded (TTL) formats. A signature control feature may be enabled for any IRIG output. Signature control removes the modulation code when a Time Sync Alarm is asserted.

IRIG FORMAT: Choose the format, level and carrier desired.

IRIG AMP CONTROL: The peak-to-peak output voltage level into a 600 ohm load is adjusted by entering a digital control value in this field. The level adjustment has no effect on TTL outputs, only on AM formats. Figure 3-38 shows typical output levels for digital control values from 0 – 255.

NOTE: These are nominal values only. Actual values will vary from unit to unit. To adjust the level precisely, connect an oscilloscope to the output connector when adjusting.

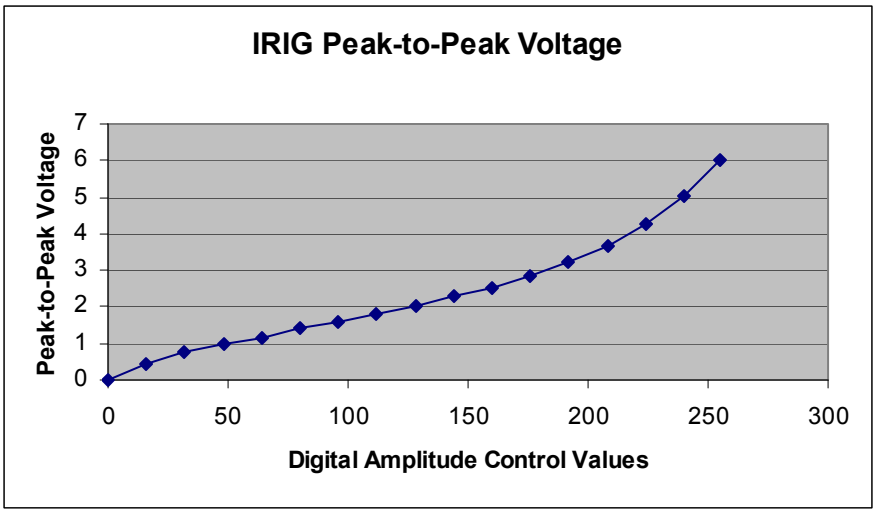


Figure 3-38: IRIG Output Level

IRIG SIGNATURE: When set to Sync, the modulation is removed when the Time Sync Alarm is asserted. When set to None, the modulation will be present even if the Time Sync Alarm is asserted.

For reference, detailed information about the IRIG B and IRIG E formats follows.
.

3.4.3.1 IRIG B Output

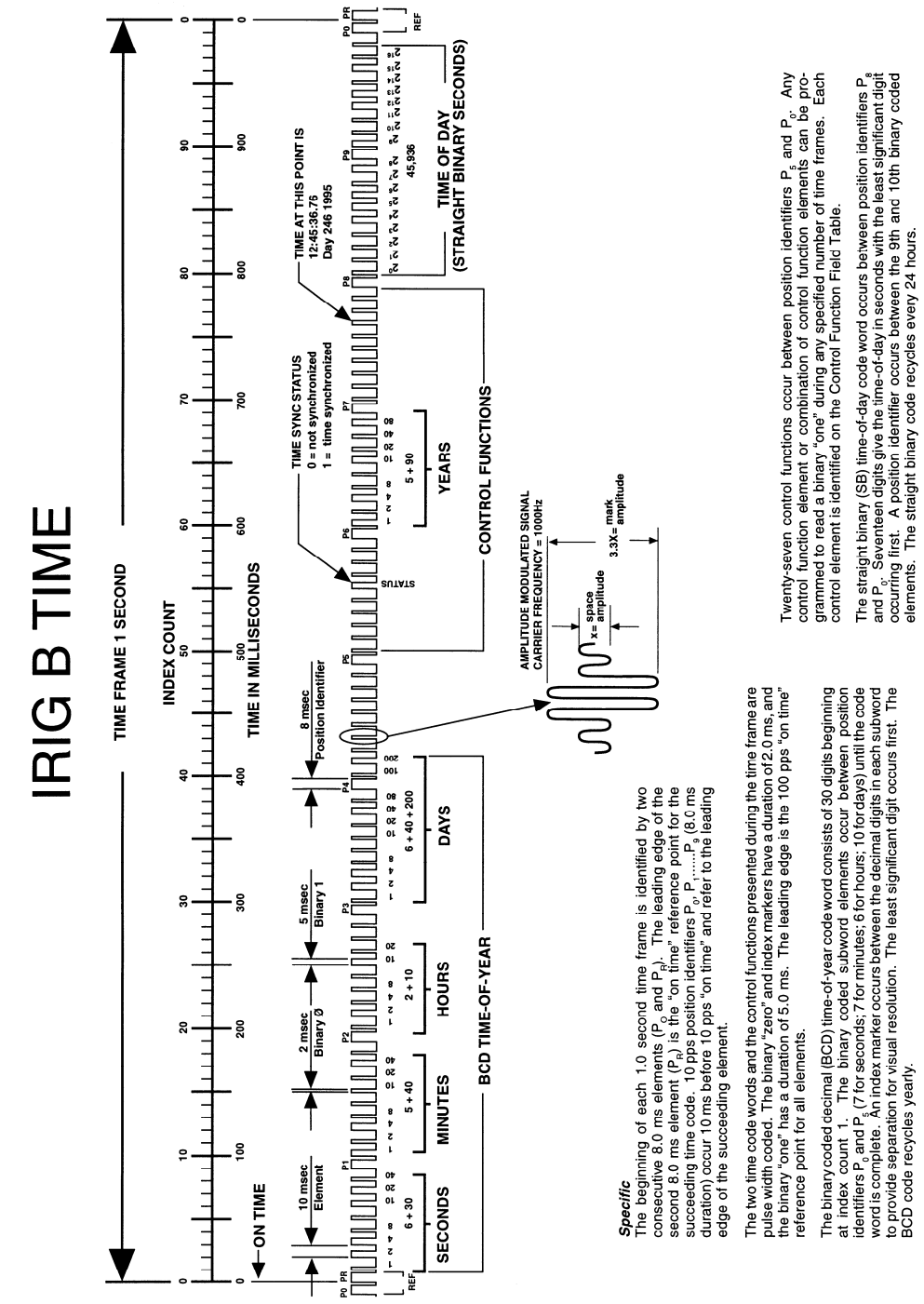

IRIG B TIME
TIME FRAME 1 SECOND
INDEX COUNT
TIME IN MILLISECONDS
ON TIME
10 msec Element
2 msec Binary Ø
5 msec Binary 1
8 msec Position Identifier
SECONDS
MINUTES
HOURS
DAYS
BCD TIME-OF-YEAR
TIME SYNC STATUS
0 = not synchronized
1 = time synchronized
TIME AT THIS POINT IS
12:45:36.76
Day 246 1995
45,936
TIME OF DAY
(STRAIGHT BINARY SECONDS)
YEARS
CONTROL FUNCTIONS
AMPLITUDE MODULATED SIGNAL
CARRIER FREQUENCY = 1000Hz
x= space amplitude
3.3X= mark amplitude
Specific
The beginning of each 1.0 second time frame is identified by two consecutive 8.0 ms elements (P_0 and P_R). The leading edge of the second 8.0 ms element (P_R) is the "on time" reference point for the succeeding time code. 10 pps position identifiers P_0, P_1.....P_9 (8.0 ms duration) occur 10 ms before 10 pps "on time" and refer to the leading edge of the succeeding element.
The two time code words and the control functions presented during the time frame are pulse width coded. The binary "zero" and index markers have a duration of 2.0 ms, and the binary "one" has a duration of 5.0 ms. The leading edge is the 100 pps "on time" reference point for all elements.
The binary coded decimal (BCD) time-of-year code word consists of 30 digits beginning at index count 1. The binary coded subword elements occur between position identifiers P_0 and P_5 (7 for seconds; 7 for minutes; 6 for hours; 10 for days) until the code word is complete. An index marker occurs between the decimal digits in each subword to provide separation for visual resolution. The least significant digit occurs first. The BCD code recycles yearly.
Twenty-seven control functions occur between position identifiers P_5 and P_0. Any control function element or combination of control function elements can be programmed to read a binary "one" during any specified number of time frames. Each control element is identified on the Control Function Field Table.
The straight binary (SB) time-of-day code word occurs between position identifiers P_8 and P_0. Seventeen digits give the time-of-day in seconds with the least significant digit occurring first. A position identifier occurs between the 9th and 10th binary coded elements. The straight binary code recycles every 24 hours.

Figure 3-39: IRIG B Time Code description

The IRIG B code contains the Binary Coded Decimal (BCD) time of year, Control Function (CF) field and the Straight Binary Seconds time of day. The following figure illustrates the IRIG B data structure. The BCD time of year provides the day of the year, 1-366, and the time of day including seconds. The hour of the day is expressed in 24 hour format. The SBS time is the number of seconds elapsed since midnight. The Control Function field contains year information and a time synchronization status bit.

1. Time frame: 1.0 seconds.
2. Code digit weighting:
   - A. Binary Coded Decimal time-of-year.
     Code word - 30 binary digits.
     Seconds, minutes hours, and days.
     Recycles yearly.

   - B. Straight Binary Seconds time-of-day.
     Code word - 17 binary digits.
     Seconds only, recycles daily.
3. Code word structure:

BCD: Word seconds digits begin at index count 1. Binary coded elements occur between position identifier elements P_0 and P_5 (7 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.

CF: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG B has 27 Control Functions located between elements 50 and 78. The NetClock uses the Control Functions to encode year information and time synchronization status.

Table 3-3 lists the Control Function Field and each element's function.

Element 55 is the time synchronization status bit. Element 55 is a Binary 1 when the front panel time synchronization lamp is green, and a Binary 0 when the lamp is red.

Year information consists of the last two digits of the current year (i.e. 97, 98, 99 etc.). Elements 60 through 63 contain the binary equivalent of year units. Elements 65 through 68 contain the binary equivalent of tens of years. In keeping with IRIG formats, the least significant bit occurs first. All unused Control Functions are filled with a space (Binary 0).

SBS: Word begins at index count 80. Seventeen Straight Binary Coded elements occur with a position identifier between the 9th and 10th binary coded elements. Least significant digit occurs first.

4. Pulse rates:
Element rate: 100 per second.
Position identifier rate: 10 per second.
Reference marker rate: 1 per second.

5. Element identification: The "on time" reference point for all elements is the pulse leading edge.

Index marker (Binary 0 or uncoded element): 2 millisecond duration.
Code digit (Binary 1): 5 millisecond duration.
Position identifier: 8 millisecond duration.
Reference marker, 1 per second. The reference marker appears as two consecutive position identifiers. The second position identifier marks the on-time point for the succeeding code word.

6. Resolution:
   Pulse width coded signal: 10 milliseconds.
   Amplitude modulated signal: 1 millisecond.

7. Carrier frequency: 1 kHz when modulated.

C.F. ELEMENT #	DIGIT #	FUNCTION
50	1	Space
51	2	Space
52	3	Space
53	4	Space
54	5	Space
55	6	Time Sync Status
56	7	Space
57	8	Space
58	9	Space
59	PID P6	Position Identifier
60	10	Years Units Y1
61	11	Years Units Y2
62	12	Years Units Y4
63	13	Years Units Y8
64	14	Space
65	15	Years Tens Y10
66	16	Years Tens Y20
67	17	Years Tens Y40
68	18	Years Tens Y80
69	PID P7	Position Identifier
70	19	Space
71	20	Space
72	21	Space
73	22	Space
74	23	Space
75	24	Space
76	25	Space
77	26	Space
78	27	Space

Table 3-3: IRIG B Control Function Field

3.4.3.2 IRIG E Output

The IRIG E code contains the Binary Coded Decimal (BCD) time of year and Control Functions.

Figure 3-40 illustrates the IRIG E data structure. The BCD time of year provides the day of year, 1-366, and time of day to tens of seconds. The hour of the day is expressed in 24 hour format.

The Control Function field includes a time synchronization status bit, year information and SBS time of day.

1. Time frame: 10 seconds.

2. Code Digit Weighting:
   Binary Coded Decimal time of year.
   Code world - 26 binary digits.
   Tens of seconds, minutes, hours, and days.
   Recycles yearly.

3. Code Word Structure: BCD word tens of seconds digits begin at index count 6. Binary coded elements occur between position identifier elements P_0 and P_5 (3 for seconds, 7 for minutes, 6 for hours, and 10 for days) until the code word is complete. An index marker occurs between decimal digits in each group to provide separation for visual resolution. Least significant digit occurs first.

4. Control Functions: IRIG formats reserve a set of elements known as Control Functions (CF) for the encoding of various control, identification, or other special purpose functions. IRIG E has 45 Control Functions located between elements 50 and 98. The NetClock uses the Control Function field to encode year data, time synchronization status, and SBS time data. Table B-2 lists the Control Function Field and each element's function.

Element 55 is the time synchronization status bit. Element 55 is a Binary 1 when the front panel time synchronization lamp is green, and a Binary 0 when the lamp is red.

Year information consists of the last two digits of the current year (i.e. 98, 99, etc.). Elements 60 through 63 contain the binary equivalent of year units. Elements 65 through 68 contain the binary equivalent of tens of years. In keeping with IRIG formats, the least significant bit occurs first.

Elements 80 through 97 are encoded with the Straight Binary Seconds (SBS) time data. The SBS time data is incremented in 10-second steps and recycles every 24 hours.

5. Pulse rates:
   A. Element rate: 10 per second.
   B. Position identifier rate: 1 per second.
   C. Reference marker rate: 1 per 10 seconds.

6. Element identification: The "on time" reference point for all elements is the pulse leading edge.

Index marker (Binary 0 or uncoded element): 20 millisecond duration.
Code digit (Binary 1): 50 millisecond duration.
Position identifier: 80 millisecond duration.
Reference marker: 80 millisecond duration, 1 per 10 seconds. The reference marker appears as two consecutive position identifiers. The second position identifier or reference marker is the on-time point for the succeeding code word.

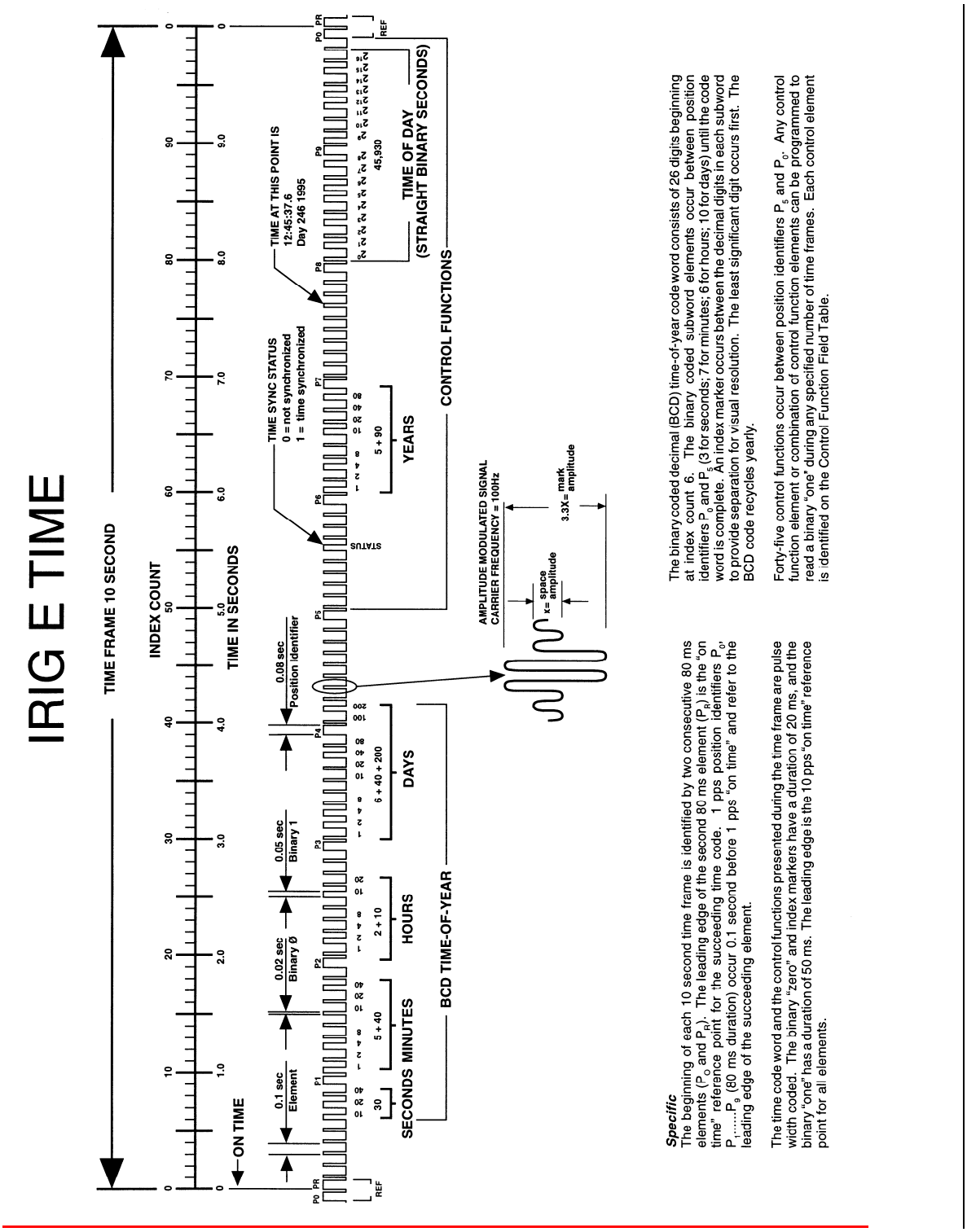

IRIG E TIME
TIME FRAME 10 SECOND
INDEX COUNT
TIME IN SECONDS
ON TIME
0.1 sec Element
0.02 sec Binary Ø
0.05 sec Binary 1
0.08 sec Position Identifier
SECONDS
MINUTES
HOURS
DAYS
BCD TIME-OF-YEAR
TIME SYNC STATUS
0 = not synchronized
1 = time synchronized
STATUS
TIME AT THIS POINT IS
12:45:37.6
Day 246 1995
45,930
TIME OF DAY
(STRAIGHT BINARY SECONDS)
YEARS
CONTROL FUNCTIONS
AMPLITUDE MODULATED SIGNAL
CARRIER FREQUENCY = 100Hz
space amplitude
3.3X= mark amplitude
REF
Specific
The beginning of each 10 second time frame is identified by two consecutive 80 ms elements (P_o and P_R). The leading edge of the second 80 ms element (P_R) is the "on time" reference point for the succeeding time code. 1 pps position identifiers P_0, P_1.....P_9 (80 ms duration) occur 0.1 second before 1 pps "on time" and refer to the leading edge of the succeeding element.
The time code word and the control functions presented during the time frame are pulse width coded. The binary "zero" and index markers have a duration of 20 ms, and the binary "one" has a duration of 50 ms. The leading edge is the 10 pps "on time" reference point for all elements.
The binary coded decimal (BCD) time-of-year code word consists of 26 digits beginning at index count 6. The binary coded subword elements occur between position identifiers P_0 and P_5 (3 for seconds; 7 for minutes; 6 for hours; 10 for days) until the code word is complete. An index marker occurs between the decimal digits in each subword to provide separation for visual resolution. The least significant digit occurs first. The BCD code recycles yearly.
Forty-five control functions occur between position identifiers P_5 and P_0. Any control function element or combination of control function elements can be programmed to read a binary "one" during any specified number of time frames. Each control element is identified on the Control Function Field Table.

Figure 3-40: IRIG E Time Code Description

BIT #	CF ELEMENT #	FUNCTION
50	1	SPACE
51	2	SPACE
52	3	SPACE
53	4	SPACE
54	5	SPACE
55	6	TIME SYNC STATUS
56	7	SPACE
57	8	SPACE
58	9	SPACE
59	PID P6	POSITION IDENTIFIER
60	10	YEAR UNITS Y1
61	11	YEAR UNITS Y2
62	12	YEAR UNITS Y4
63	13	YEAR UNITS Y8
64	14	SPACE
65	15	YEAR TENS Y10
66	16	YEAR TENS Y20
67	17	YEAR TENS Y40
68	18	YEAR TENS Y80
69	PID P7	POSITION IDENTIFIER
70	19	SPACE
71	20	SPACE
72	21	SPACE
73	22	SPACE
74	23	SPACE
75	24	SPACE
76	25	SPACE
77	26	SPACE
78	27	SPACE
79	PID P8	POSITION IDENTIFIER
80	28	SBS 2^0
81	29	SBS 2^1
82	30	SBS 2^2
83	31	SBS 2^3
84	32	SBS 2^4
85	33	SBS 2^5
86	34	SBS 2^6
87	35	SBS 2^7
88	36	SBS 2^8
89	PID P9	POSITION IDENTIFIER
90	37	SBS 2^9
91	38	SBS 2^{10}
92	39	SBS 2^{11}
93	40	SBS 2^{12}
94	41	SBS 2^{13}
95	42	SBS 2^{14}
96	43	SBS 2^{15}
97	44	SBS 2^{16}
98	45	SPACE
99	PID P0	POSITION IDENTIFIER

Table 3-4: IRIG E Control Function Field

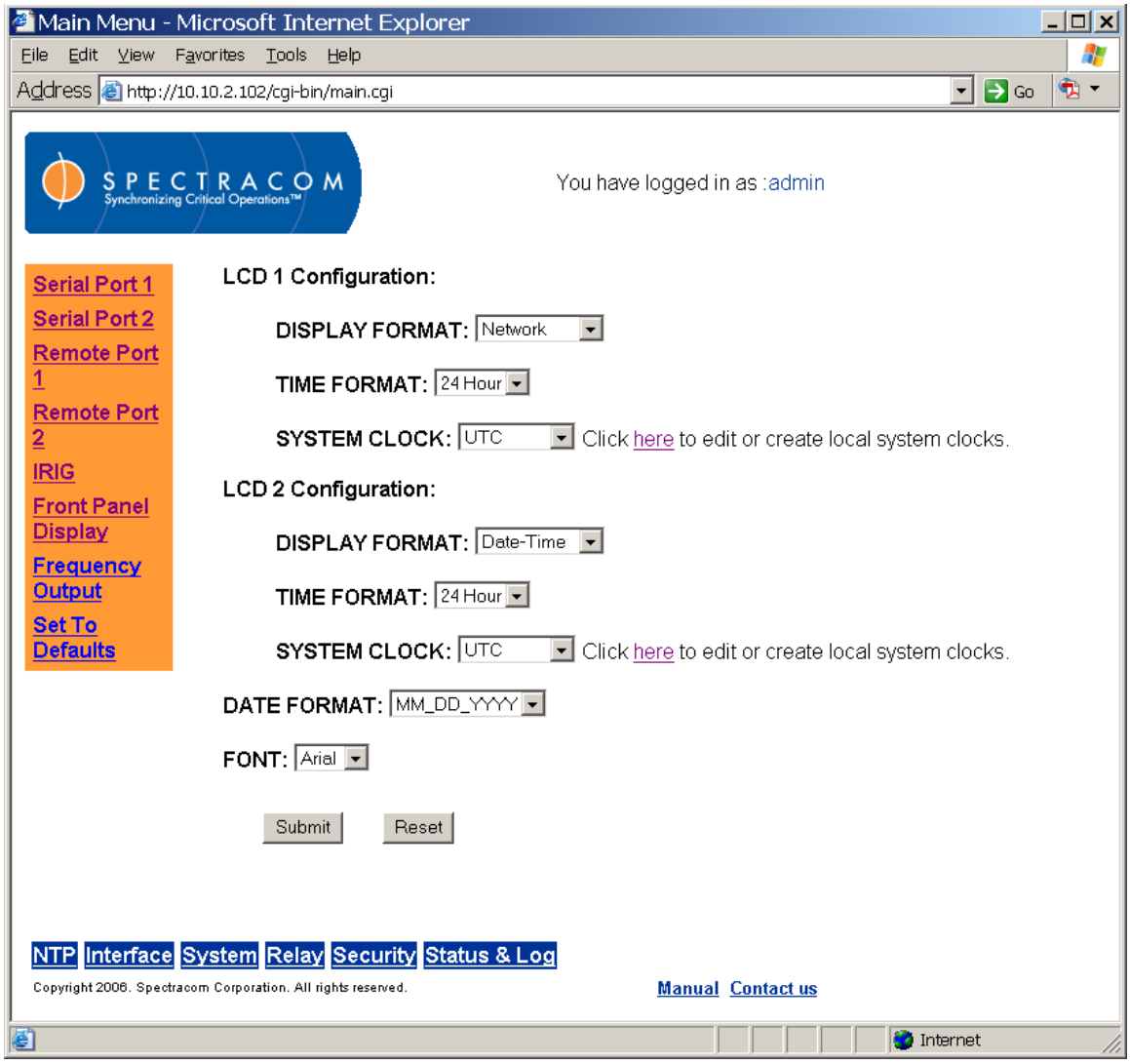


Figure 3-41: Interface Front Panel Display Screen

The NetClock has two front panel displays that are independently programmable. The left display is LCD 1 and the right display is LCD 2. You may use the Web UI to change the display and time format and to select (or edit, or create) system clocks. The display font may also be changed (and includes a custom font, named “Mark.”) When you make a change to the front panel display configuration and click “Submit,” the change in the display is immediately visible on the front panel.

NOTE: When selecting a system clock to display on one LCD of the front panel LCDs, while displaying the date on the other LCD, be sure to use the same system clock in both display. If setting the time to local time, change the date to local time as well. Otherwise, the “new day” time and the “new date” rollover may not coincide with each other.

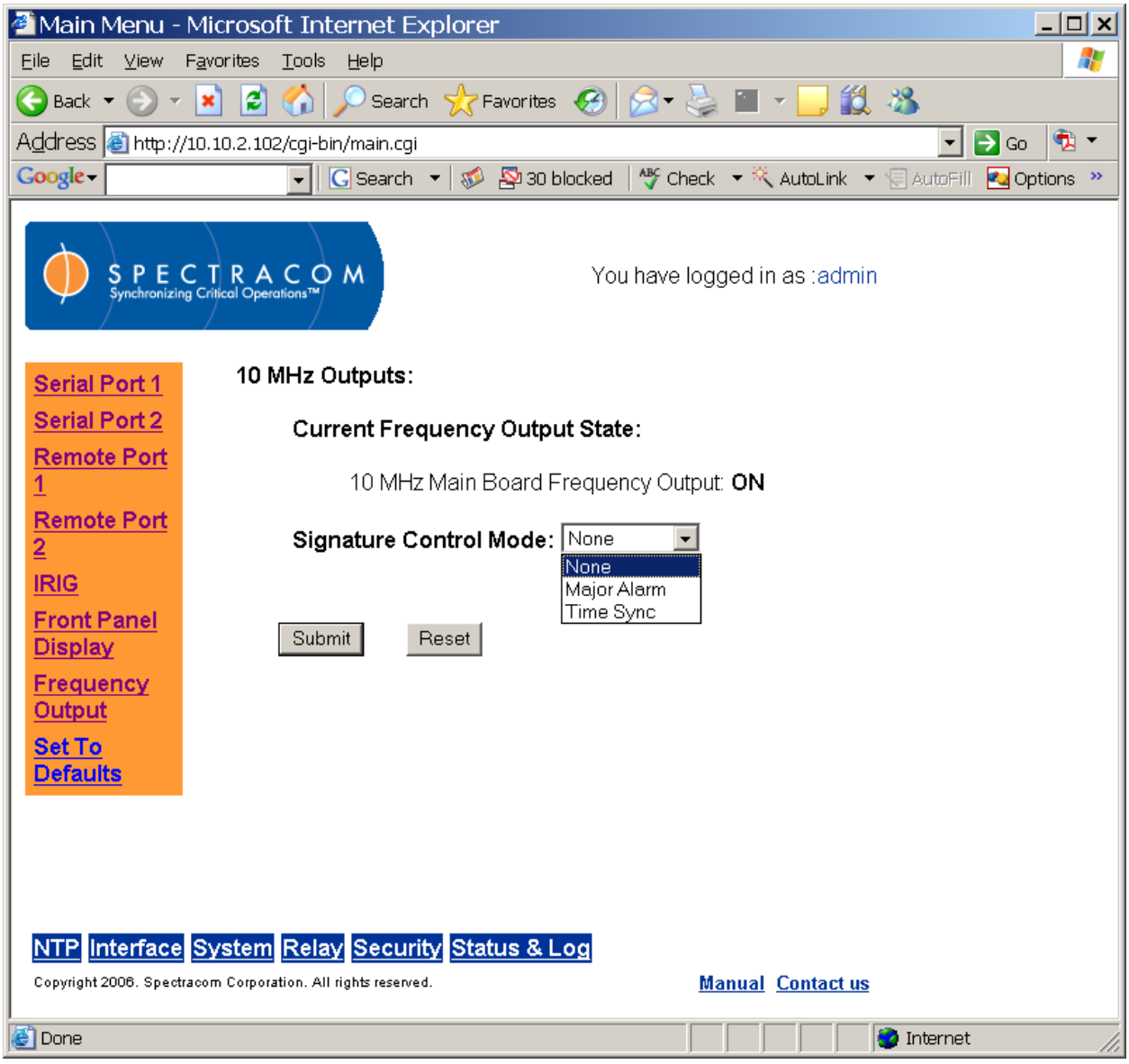


Figure 3-42: Interface Frequency Output Screen

The rear panel 10 MHz output can be disabled in the event of an alarm condition or loss of time synchronization. This feature is known as signature control. From the Interface Frequency Output screen (Figure 3-42), the user may select from three signature control outputs:

None: 10 MHz output continues regardless of alarm condition.
Major Alarm: 10 MHz output stops if the NetClock experiences a major alarm.
Time Sync: 10 MHz output stops if the NetClock loses time synchronization.

NOTE: Oscillator disciplining depends on a very stable reference 1PPS input signal. Because of this, the Modem dial-out option (Option 03) available for the 9300 Series cannot be used for oscillator disciplining and hence does not result in enabling 10MHz frequency outputs when time synchronization is achieved using these time sources. The NetClock must be synchronized to GPS with a 3-D fix (minimum of four satellites)

when the 10 MHz output must be disciplined for accuracy. Without a 3-D fix present and with signature control set to “None,” the frequency output will always be present but not disciplined for accuracy.

Because a window-mounted antenna will have difficulties maintaining at least four satellites continuously, the window-mount antenna, Model 8228, should not be used when disciplining of the 10 MHZ is desired. The antenna must be installed outdoors with a good view of the horizon.

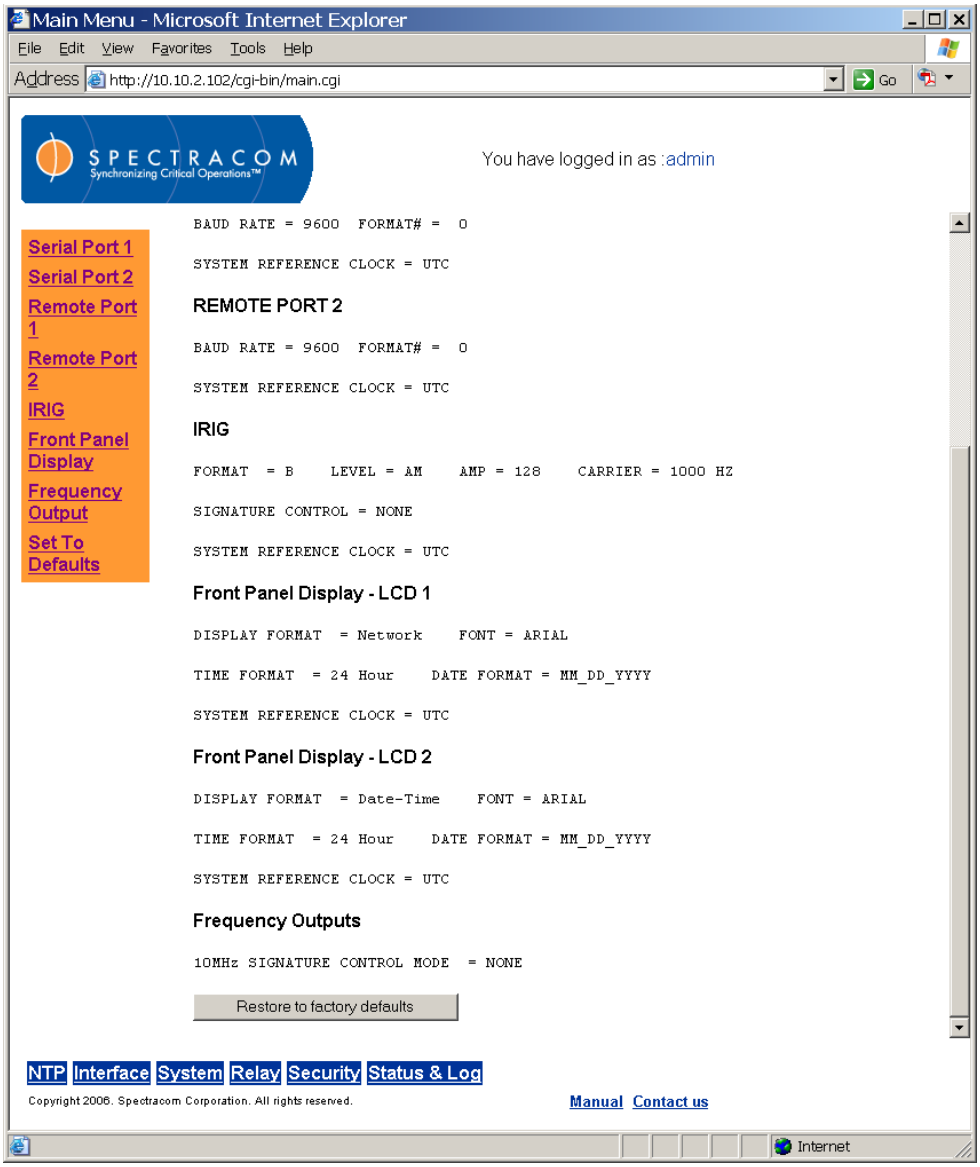

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Serial Port 1
Serial Port 2
Remote Port 1
Remote Port 2
IRIG
Front Panel Display
Frequency Output
Set To Defaults
BAUD RATE = 9600 FORMAT# = 0
SYSTEM REFERENCE CLOCK = UTC
REMOTE PORT 2
BAUD RATE = 9600 FORMAT# = 0
SYSTEM REFERENCE CLOCK = UTC
IRIG
FORMAT = B LEVEL = AM AMP = 128 CARRIER = 1000 HZ
SIGNATURE CONTROL = NONE
SYSTEM REFERENCE CLOCK = UTC
Front Panel Display - LCD 1
DISPLAY FORMAT = Network FONT = ARIAL
TIME FORMAT = 24 Hour DATE FORMAT = MM_DD_YYYY
SYSTEM REFERENCE CLOCK = UTC
Front Panel Display - LCD 2
DISPLAY FORMAT = Date-Time FONT = ARIAL
TIME FORMAT = 24 Hour DATE FORMAT = MM_DD_YYYY
SYSTEM REFERENCE CLOCK = UTC
Frequency Outputs
10MHz SIGNATURE CONTROL MODE = NONE
Restore to factory defaults
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Internet

Figure 3-43: Interface Set to Defaults Screen

From the Interface Set to Defaults screen (Figure 3-43), the user may click the “Restore to factory defaults” button to set the Interface values (and the Interface values ONLY) to the factory settings.

3.4.4 Sysplex Timing

The NetClock may be used as an external time source (ETS) to synchronize an IBM Sysplex Timer. This is achieved by configuring Serial Port 1 (refer to *Configuring the Interface*) on the NetClock to the following settings (Figure 3-44):

Baud Rate: 9600
Data Format: 02
Request Char: User-defined, 'T'
System Clock: UTC

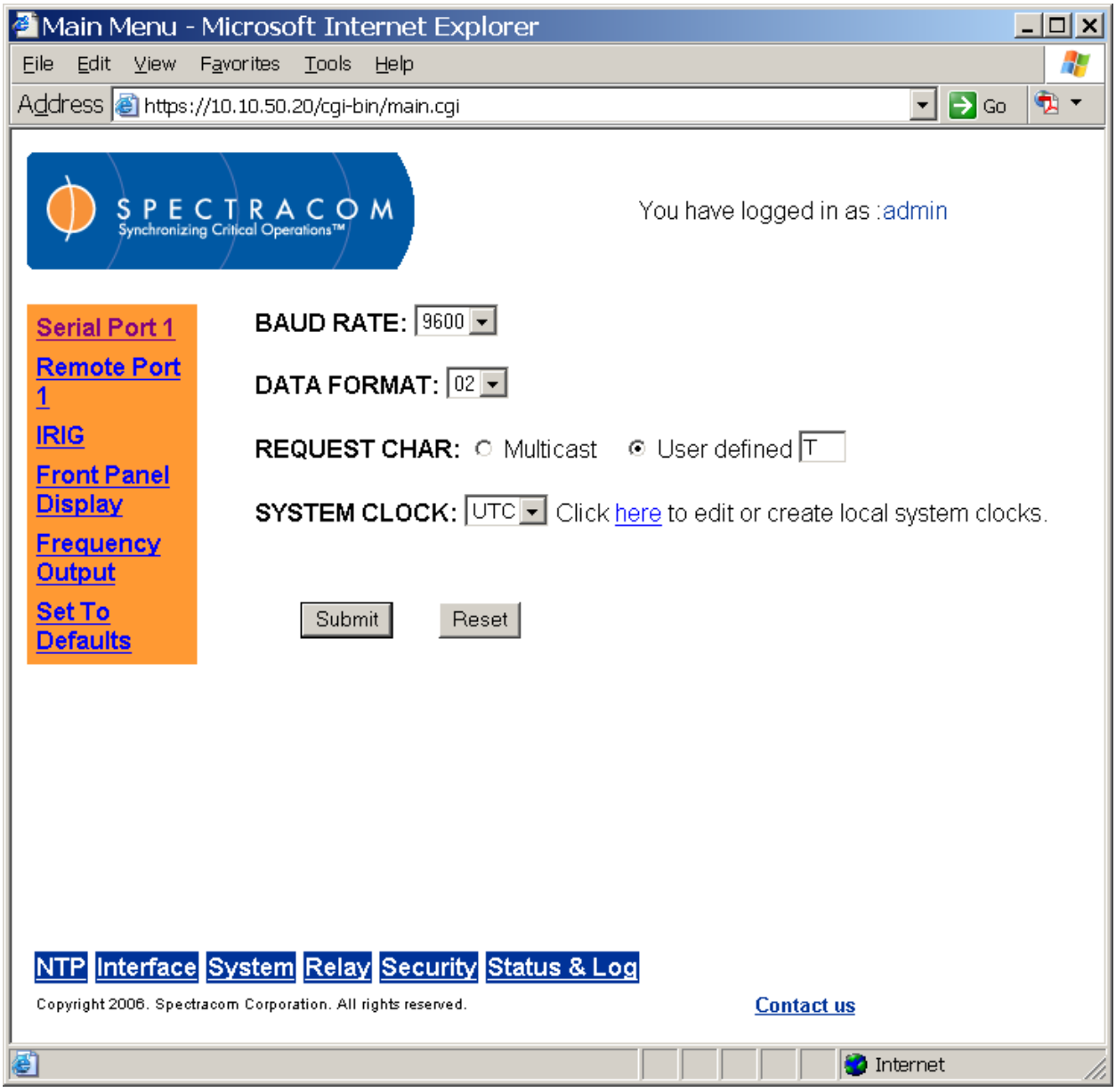


Figure 3-44: Configuring Serial Port 1 for Sysplex Timing

The Sysplex Timer must be configured to use Protocol 2 (NetClock/2) and connected to the NetClock Serial Comm 1 port via a 9-pin serial cable (not included). Older Sysplex Timers (9037-001) may connect to an ETS through the Sysplex Timer's console port, while later model Sysplex Timers (9037-002) feature a dedicated ETS port.

3.4.5 Configuring the System: SNMP

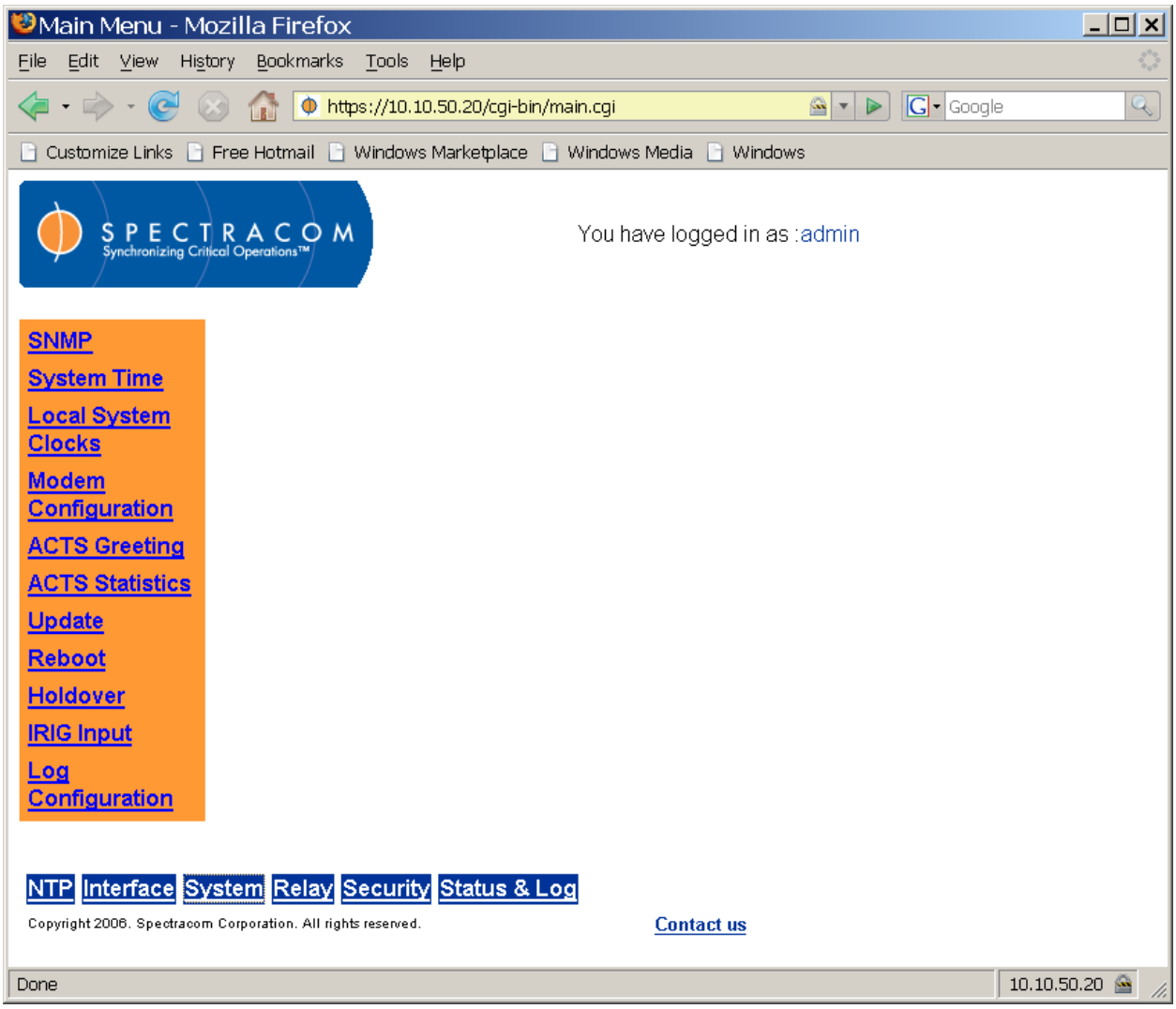


Figure 3-45: System Menu

The System menu groups the NetClock's various system configuration functions (Figure 3-45). From this menu, the user may access screens for SNMP, Alarms, GPS, System Time, Local System Clocks, System mode, Modem Configuration (if the NetClock includes the modem option), Reboot, Holdover, and Log Configuration.

NOTE: Refer to *Options* for modem configuration and related screens. If your NetClock does not have the modem option (which is activated at the factory), the modem menu links will not appear on the System screen. If you purchase the Modem option after receipt

of your NetClock system, Spectracom will provide you with a product key for modem activation.

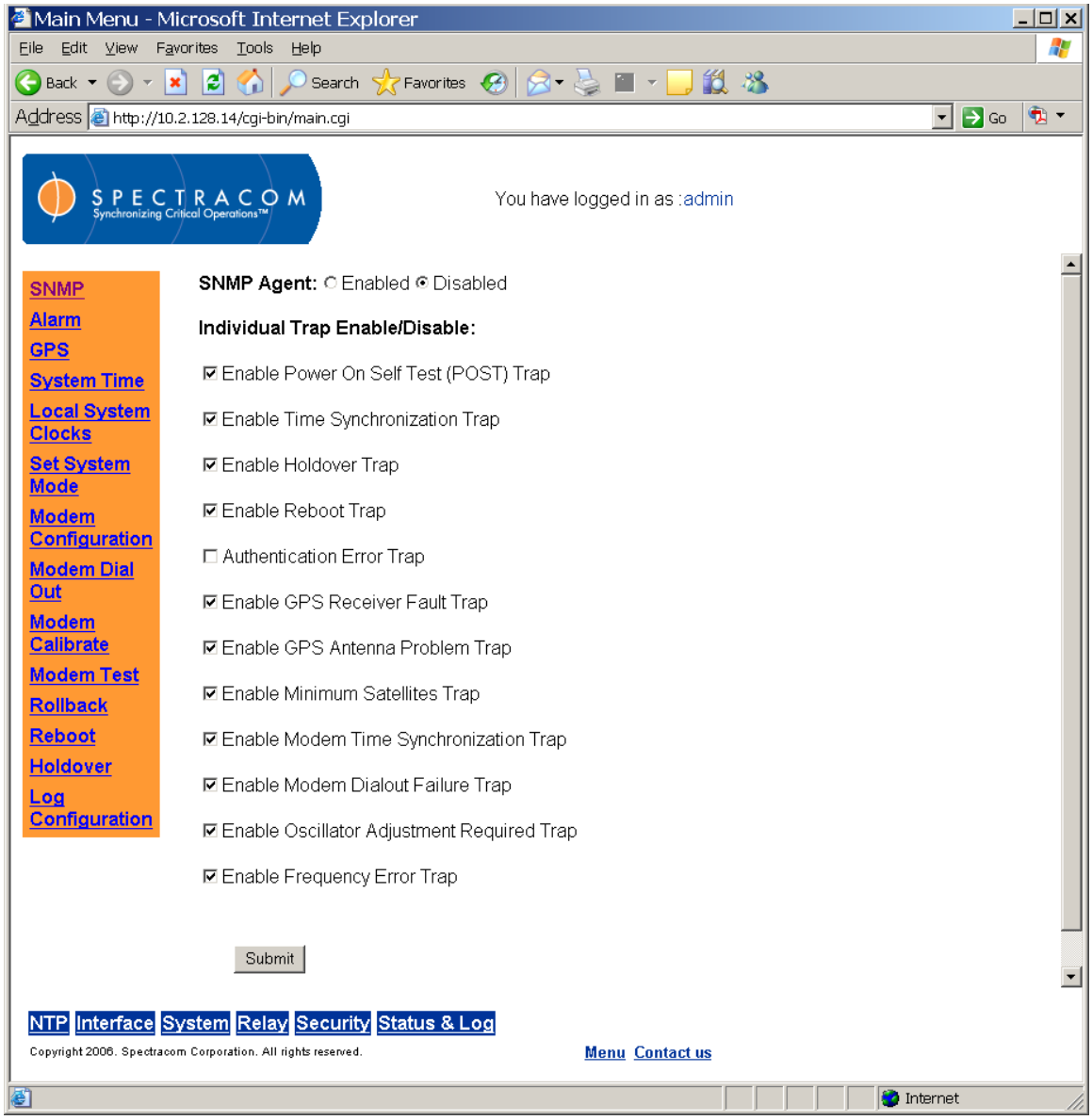


Figure 3-46: System SNMP Screen

SNMP (Simple Network Management Protocol) is a set of standards for managing network devices, which includes a protocol, a database structure specification, and a set of data objects. The communication protocol involves one or more network management stations monitoring one or more network devices. SNMP enabled devices must have an SNMP agent application that is capable of handling network management functions requested by a network manager. The agent is also responsible for controlling the database of control variables defined in the product's Management Information Base (MIB).

Click the radio buttons at the top of the System SNMP screen (Figure 3-46) to enable or disable SNMP. You may also check the boxes to enable or disable individual traps. (Traps are

asynchronous status messages sent from NetClock to the locations specified in the SNMP security screens.)

3.4.5.1 Spectracom MIB

Spectracom has been assigned the enterprise identifier 18837 by the IANA (Internet Assigned Numbers Authority). Spectracom's MIB for its time and frequency products resides under this enterprise identifier @ 18837.3.1 which is illustrated below.

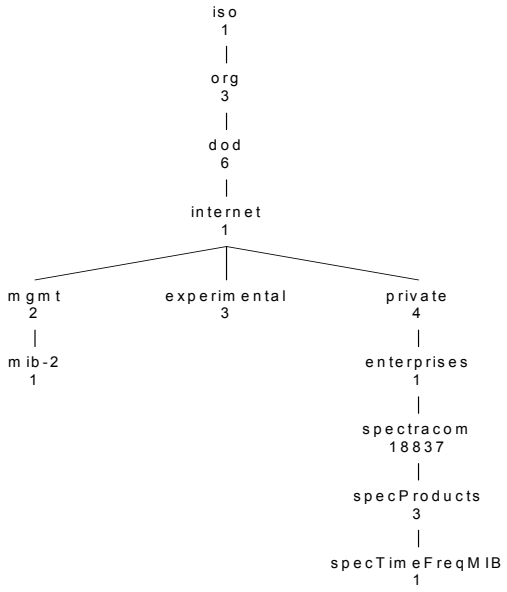


Figure 3-47: Spectracom's MIB

3.4.5.2 SNMP Support

Spectracom's private enterprise MIB can be obtained from the Spectracom Customer Service department via email. It can also be obtained via File Transfer Protocol (FTP) from the NetClock using an FTP agent such as Microsoft FTP, CoreFTP, or any other shareware/freeware FTP program.

To obtain the MIB file via FTP, using your FTP program, log in as an administrator and change the file transfer mode to "binary." The Spectracom MIB files are located in the /MIBS directory and include global, time-frequency, and NTPv4 files. There is a Global (generic) MIB file and a NetClock-specific MIB file called "Time and Frequency." FTP the files to the desired location on your PC for later transfer to the SNMP Manager. The MIB files may then be compiled onto the SNMP Manager.

NOTE: When compiling the MIB files, some SNMP Manager programs may require the MIB files to be named something other than the current name for the files**.** The MIB file names ("Global" and "Time and Frequency") may be changed or edited as necessary to meet the requirements of the SNMP Manager. Refer to the SNMP Manager documentation for more information on these requirements.

3.4.6 Configuring Alarms

An alarm is asserted when predefined error conditions exist AND the associated alarm has been enabled.

Through the System Alarm screen (Figure 3-48), the user may define what conditions constitute Major and Minor alarm conditions. These are the only user-defined NetClock Alarms. Clicking the check box to the left of a particular user-defined alarm will enable that alarm condition. Each alarm condition may be set to exist for a specified duration before activating the alarm. This is done by filling in the Timeout fields directly beneath the alarm condition.

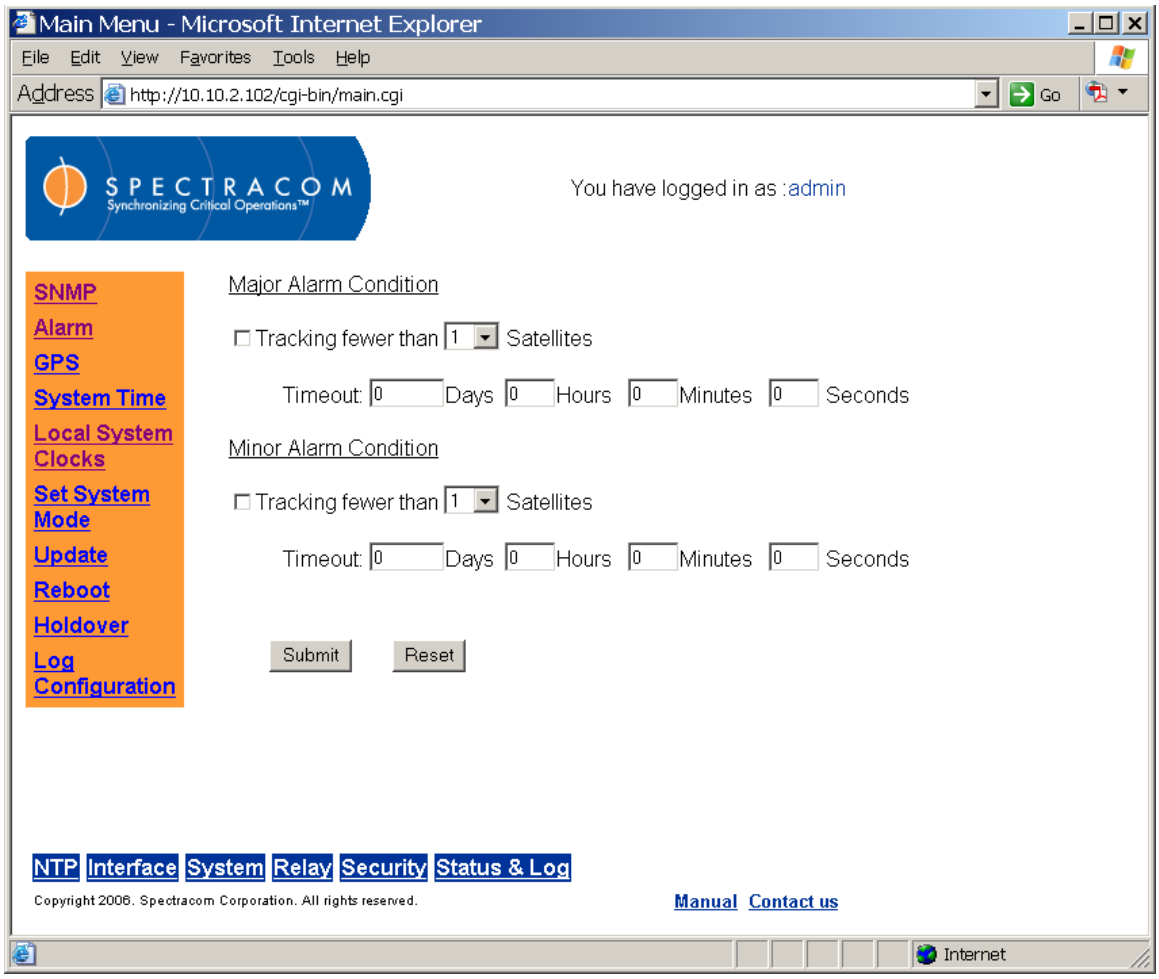


Figure 3-48: System Alarm Screen

User-defined Alarm: The user-specified period of time allotted for operation while tracking less than a user-specified number of satellites has expired. This can be a Major and/or Minor alarm.

Software Fault: One or more software sub-systems have experienced a major run-time error. This is a Major alarm.

Time Sync Alarm: The period of time allotted for operation without tracking sufficient qualified satellites has expired. The factory default period is 2 hours. This is a Major alarm.

GPS Receiver Fault: The CPU cannot communicate with the GPS receiver. This is a Major alarm.

Frequency Error: Measured oscillator frequency error exceeds limits (Table 3-5). This is a Major alarm.

Oscillator	Option	Frequency Limit
TCXO	Standard	6.6×10^{-9}
OCXO	Option 05	6.6×10^{-10}
Rb	Option 04	3.3×10^{-10}

Table 3-5: Oscillator Frequency Error Limits

Power Failure: The NetClock has lost power. This is both a Major and a Minor alarm.

Antenna Problem: The antenna sense circuitry warns when the antenna is not connected or a cable short or open is detected. This is a Minor alarm.

Oscillator Adjust: The oscillator requires an adjustment to maintain operation within specifications. This is a Minor alarm.

3.4.7 Configuring GPS

The System GPS screen (Figure 3-49) allows the user to configure the GPS receiver to provide more accurate results and faster start up. Provided the GPS antenna is properly connected, however, it is not necessary to change the factory default settings for the unit to receive and synchronize to GPS time.

ANTENNA CABLE DELAY: By setting the correct antenna cable delay, the on-time point is offset by the delay value to compensate for the antenna and in-line amplifier delays. Under typical conditions, the expected cable and amplifier delays are negligible. You can calculate the delay based on the manufacture's specifications.

The range of the cable delay is ± 50,000,000 nanoseconds. The default value is 0 nanoseconds and the resolution is 1 nanosecond.

The following formula is used to calculate the cable delay:

D = (L * C) / V

Where:

D = Cable delay in nanoseconds
L = Cable length in feet
C = Constant derived from velocity of light: 1.016
V = Nominal velocity of propagation expressed as decimal, i.e. %66 = 0.66 Value is provided by cable manufacturer.

NOTE: The antenna cable delay is nominal and beyond the accuracy specifications of the GPS receiver. It is not normally necessary to set the antenna cable delay.

You can read the current location of the unit calculated by the GPS receiver without logging in. The GPS receiver will automatically update this field when it has a Position Fix. Check the GPS Signal Status page (found in the Status and Logs menu). If the status is “Position Fix,” the location shown is the right location.

The location input by the user may only help to speed up the time to the first fix during the initial installation. The unit will automatically check the status of the GPS receiver after receiving the location input from the user. Based on the status of the GPS receiver, the unit will either tell the user that the GPS receiver already has finished the first fix and the input was abandoned, or send the location to the GPS receiver.

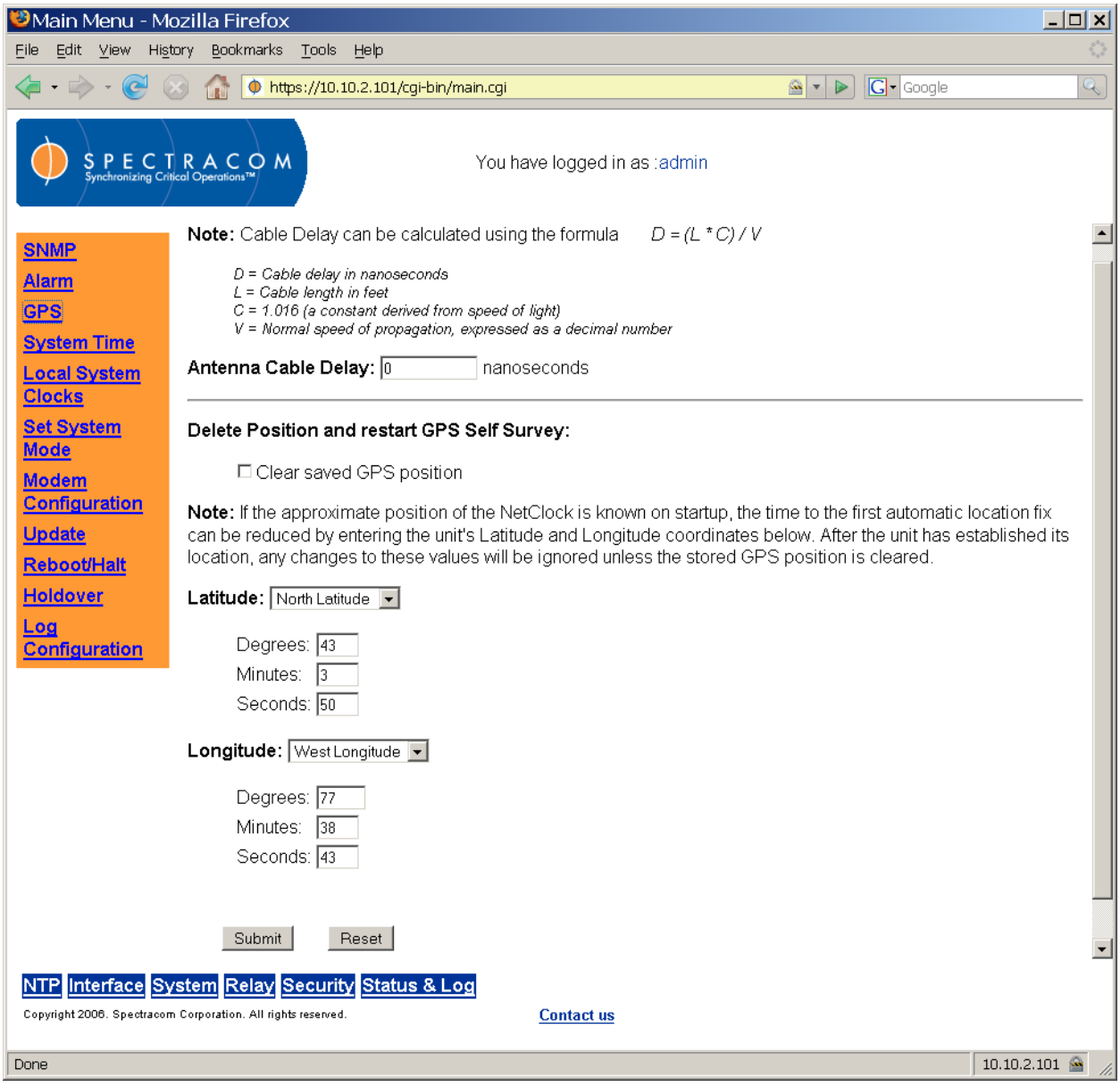

Main Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.10.2.101/cgi-bin/main.cgi
Google
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
SNMP
Alarm
GPS
System Time
Local System Clocks
Set System Mode
Modem Configuration
Update
Reboot/Halt
Holdover
Log Configuration
Note: Cable Delay can be calculated using the formula D = (L * C) / V
D = Cable delay in nanoseconds
L = Cable length in feet
C = 1.016 (a constant derived from speed of light)
V = Normal speed of propagation, expressed as a decimal number
Antenna Cable Delay: 0 nanoseconds
Delete Position and restart GPS Self Survey:
Clear saved GPS position
Note: If the approximate position of the NetClock is known on startup, the time to the first automatic location fix can be reduced by entering the unit's Latitude and Longitude coordinates below. After the unit has established its location, any changes to these values will be ignored unless the stored GPS position is cleared.
Latitude: North Latitude
Degrees: 43
Minutes: 3
Seconds: 50
Longitude: West Longitude
Degrees: 77
Minutes: 38
Seconds: 43
Submit
Reset
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Done
10.10.2.101

Figure 3-49: System GPS Screen

DELETE POSITION AND RESTART GPS SELF SURVEY: The user may delete the NetClock's GPS position and restart the GPS Self Survey on command. To ensure that no trace of position data remains on the unit, perform the following steps:

- Disconnect the NetClock's GPS antenna.
- Using the mouse, click the check box marked "Clear saved GPS position." Then click the "Submit" button. The NetClock will initiate a GPS self-survey.

3.4.8 Configuring System Time and Local Clocks

The System Time screen (Figure 3-50) allows the user to set the system time manually for test purposes or if there is no external time reference available. Setting the system time when the NetClock is connected to an external time reference will result in the external reference (for example, GPS) overriding the manually set time. The user may also view (or change) the number of leap seconds difference between UTC and GPS time.

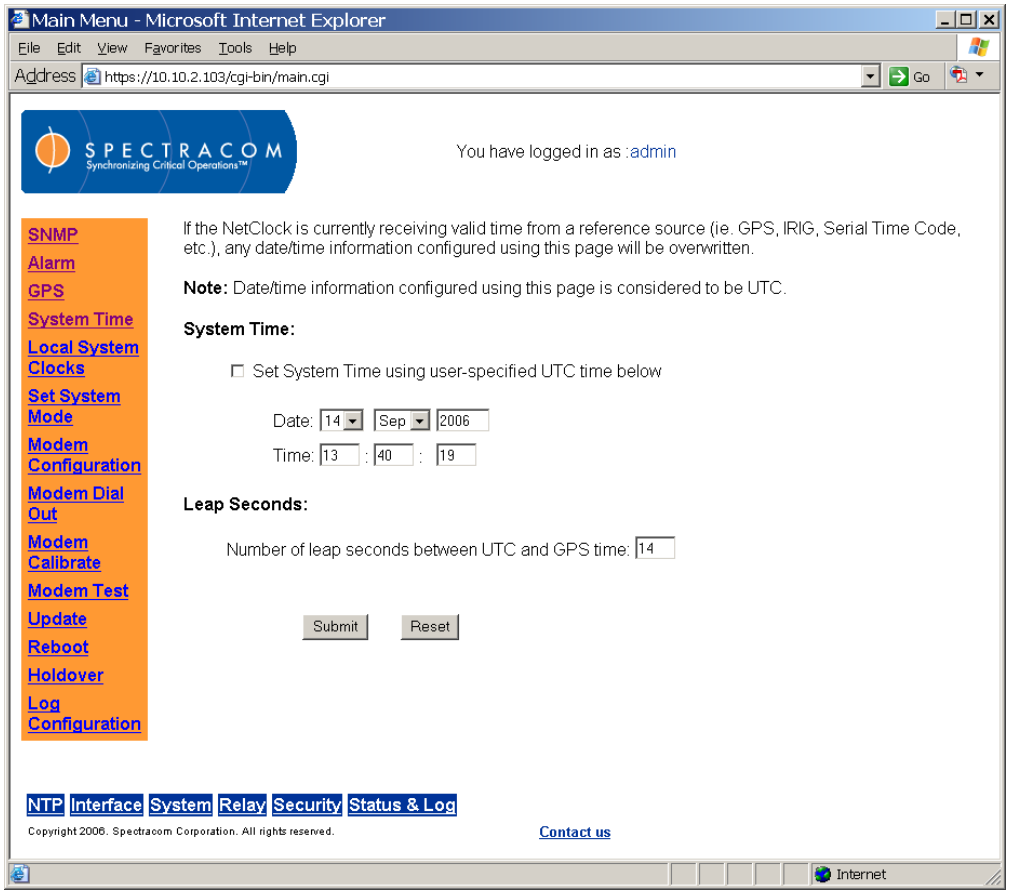

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.10.2.103/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
SNMP
Alarm
GPS
System Time
Local System Clocks
Set System Mode
Modem Configuration
Modem Dial Out
Modem Calibrate
Modem Test
Update
Reboot
Holdover
Log Configuration
If the NetClock is currently receiving valid time from a reference source (ie. GPS, IRIG, Serial Time Code, etc.), any date/time information configured using this page will be overwritten.
Note: Date/time information configured using this page is considered to be UTC.
System Time:
Set System Time using user-specified UTC time below
Date: 14 Sep 2006
Time: 13 : 40 : 19
Leap Seconds:
Number of leap seconds between UTC and GPS time: 14
Submit
Reset
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Internet

Figure 3-50: System Time Screen

When manually setting the time of the NetClock, the time is entered as UTC, not as your local time. This means the time is not corrected for either Local Time or DST correction. Entering your local time will cause an error of several hours in the NetClock outputs. The amount of error will depend on which Time Zone you are located and whether that Time Zone observers DST.

NOTE: Manually setting the time of the NetClock is not recommended unless no external reference is available to the network. When an external time reference is detected, the time and date will be changed automatically to the reference values. The manually set values will be overwritten. When this occurs, a log entry will be made in the Operational log indicating the amount of correction that was made from the manually set time. This log then shows if the time was ever manually set and then corrected by another external reference.

NOTE: Manually setting the time while synchronizing to the Option 03 modem will cause loss of time synchronization, automatically triggering a dial-out call to attempt resynchronization. Manually setting the time while synchronizing to GPS will immediately set the time to the GPS reference.

Choosing Create/New from the Local System Clocks screen Figure 3-51) allows the user to define up to five local times (times other than UTC or GPS) to display using the NetClock.

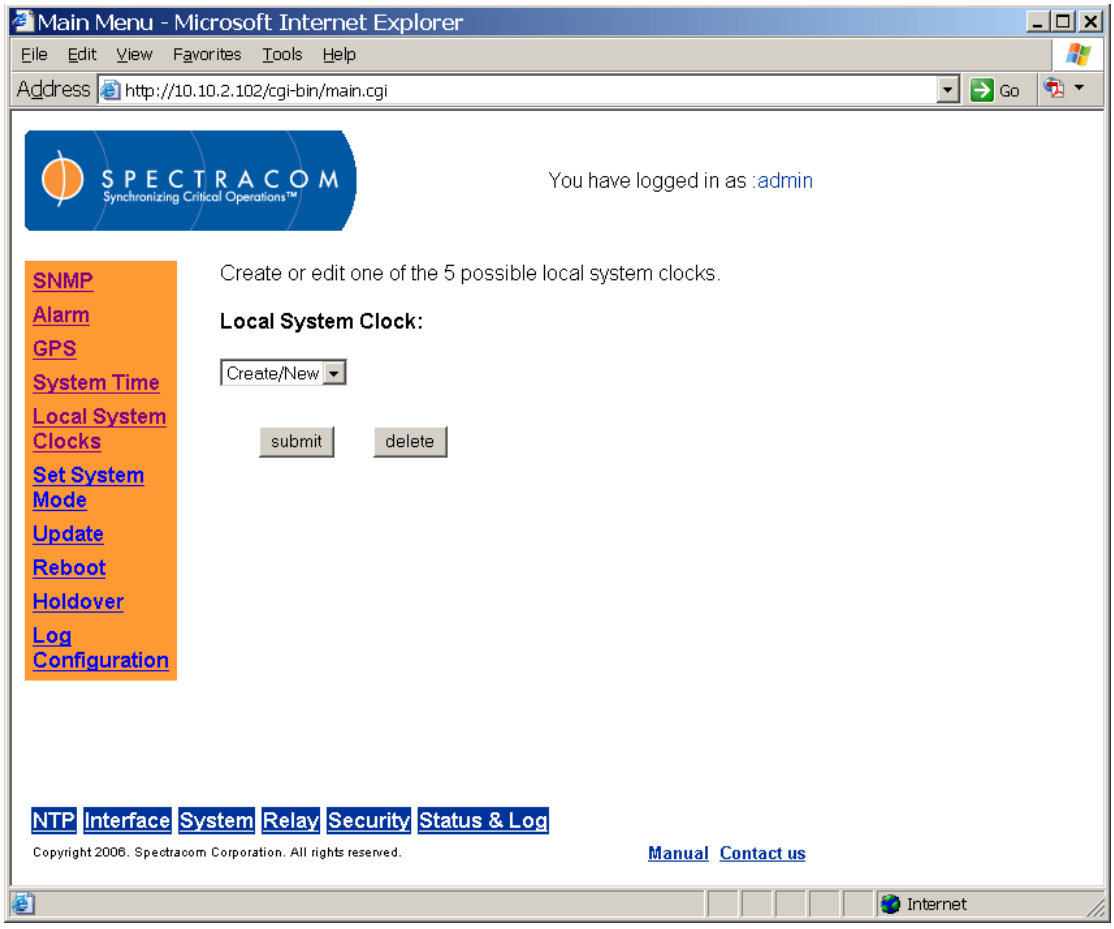


Figure 3-51: Local System Clock Screen (1 of 3)

You can define up to five local clocks or time zones to be used with any of the remote, serial, IRIG interfaces, event timers, or front panel displays.

Once defined, these local clocks can be used by any interface and will cause that interface to be automatically updated for its time zone and Daylight Saving Time (DST) conditions. To configure a local clock, perform the following steps.

NOTE: The local clock is not available from the front panel Ethernet output per the NTP specifications. NTP ALWAYS provides UTC time. Each client on the network must handle corrections for local time.

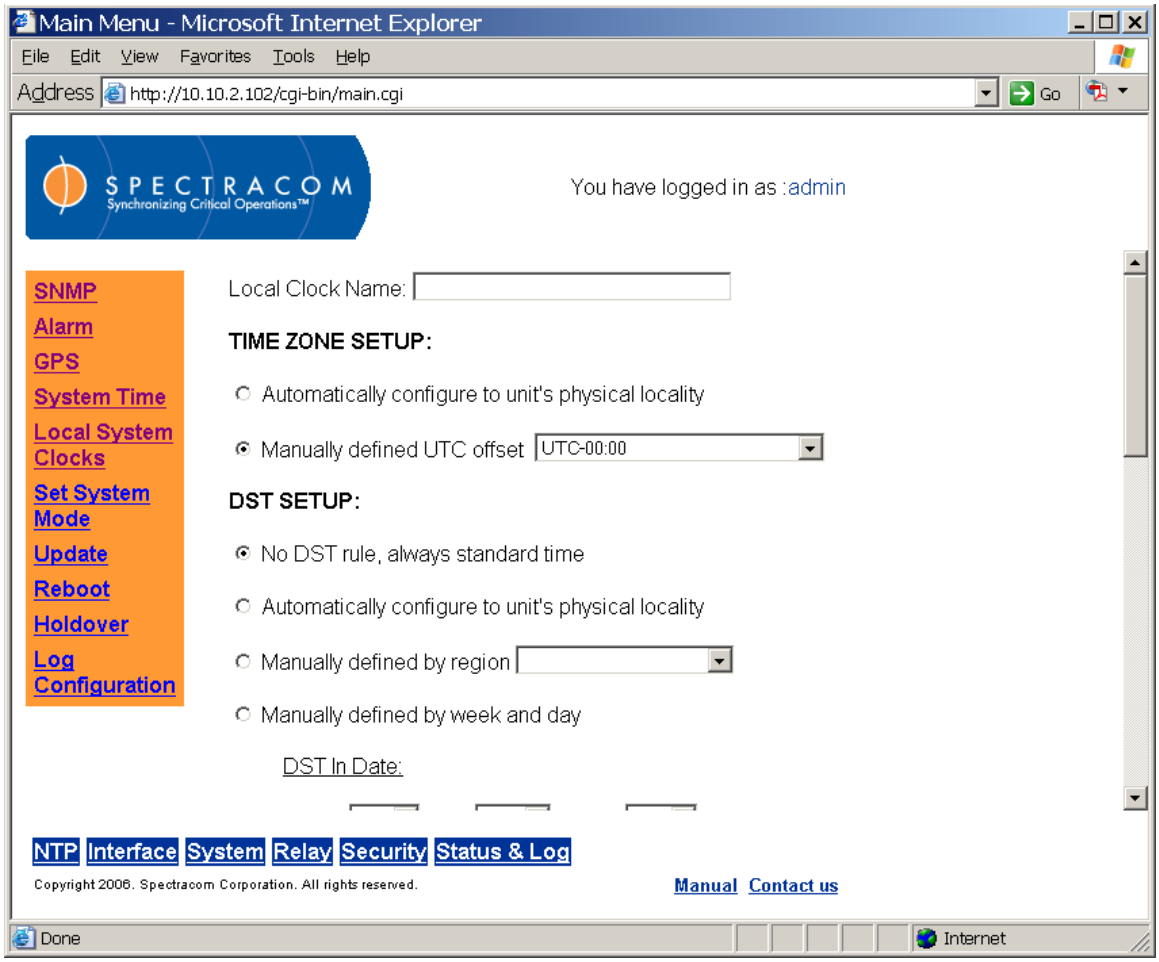


Figure 3-52: Local System Clock Screen (2 of 3)

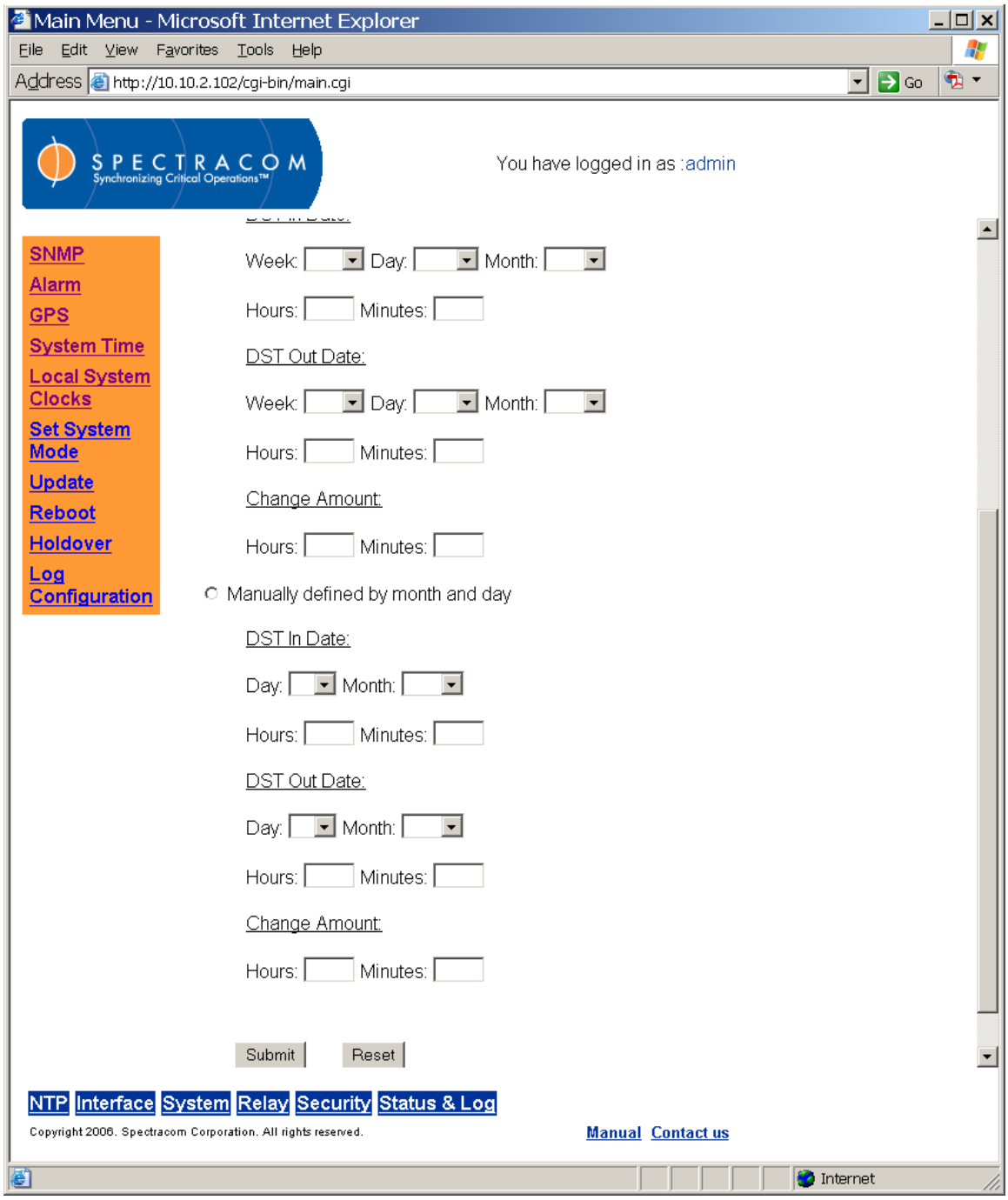


Figure 3-53: Local System Clock Screen (3 of 3)

Enter any name you wish for the Local Clock Name, up to 20 characters long. It can be any meaningful name that helps you know your point of reference (example: New York, Wall Clock in Bldg27, Eastern HQ, etc.)

TIME ZONE
Under the TIME ZONE SETUP, you will see two choices:

- Automatically configure to unit's physical locality
- Manually defined UTC offset

Automatically Configure to Unit's Physical Locality
By selecting this option, the unit will compute the Time Zone Offset automatically based on the location of the unit provided by GPS receiver.

If you select this feature before the GPS receiver completes the position calculation, a message will be displayed to explain that this feature is not valid until the position is available.

If you select this feature after the GPS receiver determines its position, the computed Time Zone Offset information will be shown.

Once this option has been selected and submitted, the NetClock software will determine the values for the appropriate manual fields. These manual definitions will be displayed when the defined clock is edited.

NOTE: Automatic time zone calculations are imprecise because the time zones are determined by local political boundaries that may change.

Manually Defined by UTC Offset
A dropdown box is provided (with definitions as appropriate) that permits the user to select a specific number of hours added or subtracted from UTC for the desired time zone.

NOTE: All of the Time Zone Offset drop-downs in the web browser user interface are configured as UTC plus or minus a set number of hours. For **Eastern**, choose UTC–5, for **Central**, choose UTC-6, for **Mountain**, choose UTC-7 and for **Pacific**, choose UTC-8.

DST SETUP
Daylight Saving Time (DST) observance varies with locality and application. Choose the configuration that reflects your location and needs. Under the DST SETUP, you will see five choices:

- No DST rule, always standard time
- Automatically configure to unit's physical locality
- Manually defined by region
- Manually defined by week and day
- Manually defined by month and day

No DST Rule, Always Standard Time
When this option is selected, the NetClock will not observe DST time changes.

Automatically Configure to Unit's Physical Locality
When this option is selected, the NetClock software will observe and implement DST time changes automatically based on the unit's physical location as determined by GPS positioning. Once this option has been selected and submitted, the NetClock software will determine the values for the appropriate manual fields. These manual definitions will be displayed when the defined clock is edited.

Manually Defined by Region
From this dropdown box, the user may select commonly defined geographic regions that share DST rules. There may be exceptions based on your location. The options include the following:

- Europe
- USA (thru 2006)
- USA (post 2006)
- Australia-1
- Australia-2

Select **Europe** if your location complies with the European DST Rule. This rule differs from all other rules because the DST changes occur based on UTC time, not local time. (All time zones in Europe change for DST at precisely the same time relative to UTC, rather than offset by local time zone.)

Select **USA (thru 2006)** if your location complies with the USA DST Rule and it is not yet the year 2007. The USA DST Rule changes in 2007.

NOTE: If you set your DST rule in 2006, you must change it manually on January 1, 2007.

Select **USA (post 2006)** if your location complies with the USA DST Rule and it is the year 2007 or later.

Select **Australia-1** if your location complies with the Australia-1 DST Rule (*Australian Capital Territory, New South Wales, South Australia, Tasmania, Victoria*).

Select **Australia-2** if your location complies with the Australia-2 DST Rule (*Western Australia*).

Manually Defined by Week and Day
This option is provided for advanced users. You can input start time, end time and the hour to change for the daylight saving. By selecting this option, the DST rule can be defined based on

the weekday, week, and month of the local time you defined for this interface. *Manual definitions are ALWAYS based on local time, not UTC.*

Manually Defined by Month and Day
This option is provided for advanced users. You can input start time, end time and the hour to change for the daylight saving. By selecting this option, the DST rule could be defined based on the day and month of the local time defined for this Interface. If you select the February 29th as the start time or end time, the unit will respond that the entry is an illegal date. *Manual definitions are ALWAYS based on local time, not UTC.*

Example 1: To create a Local System Clock to UTC+1 with no DST rule:

Select Create/New and assign the clock a meaningful name.

Click on the “Manually Defined UTC Offset” button.

Select 'UTC+1:00' from the Time Zone pull down menu.

Select the 'No DST rule' radio button.

Review the changes made and click Submit. The browser will display the status of the change.

Example 2: To configure an RS-485 port to go in DST at 2:00am on the 3rd Friday in April and out of DST at 1:00am on the 1st Sunday in October, with a DST change of 1 hour:

Select Create/New and assign the clock a meaningful name.

Under “DST Setup”, select the 'Manually defined by week and day' radio button.

Enter/select '3rd', 'Friday', 'Apr', '2', and '0' in the DST In Date section.

Enter/select '1st', 'Sunday', 'Oct', '1', and '0' in the DST Out Date section.

Enter '1' and '0' in the corresponding fields of the Change Amount section.

Review the changes made and click Submit. The browser will display the status of the change.

Browse to the “Interface Setup, Remote Port” page and Select the proper System Clock.

Example 3: To change a Local System Clock to be in DST at 1:01am on October 2nd and out of DST at 2:00am on April 17th, with a DST change of 30 minutes:

Select the desired Clock Name.

Select the 'Manually defined by month and day' radio button.

Enter/select ‘2’, ‘Oct’, ‘1’, and ‘1’ in the DST In Date section.

Enter/select ‘17’, ‘Apr’, ‘2’, and ‘0’ in the DST Out Date section.

Enter ‘0’ and ‘30’ in the corresponding fields of the Change Amount section.

Review the changes made and click Submit. The browser will display the status of the change.

The unit will allow you to define different Time Zone and DST rules for different Interfaces and a front panel display (Option 02 if so equipped). In order to use this feature properly, users have to know the correct Time Zone Offset and DST rule for your area.

The general Time Zone and DST rule information can be found from the following web sites: http://www.worldtimeserver.com/, http://webexhibits.org/daylightsaving/b.html.

3.4.9 Setting the System Mode

The user may set the system mode from the Set System Mode screen (Figure 3-54). The system supports two modes of operation. These are single satellite mode and standard mode.

Use single satellite mode if you are using a window mount antenna and cannot receive at least four satellites. This will switch the qualification algorithm used, and allow the system to operate with a fewer number of satellites, but the accuracy and capabilities of the optional Rubidium (Option 04) and OCXO (Option 05) oscillators will be decreased because of the poor GPS antenna visibility.

NOTE: Single satellite mode compromises the accuracy of the NetClock and the full capabilities of the optional OCXO and Rubidium oscillators. Always use standard mode if you are using a roof mount antenna and can obtain signals from at least four satellites. Standard mode is the factory default.

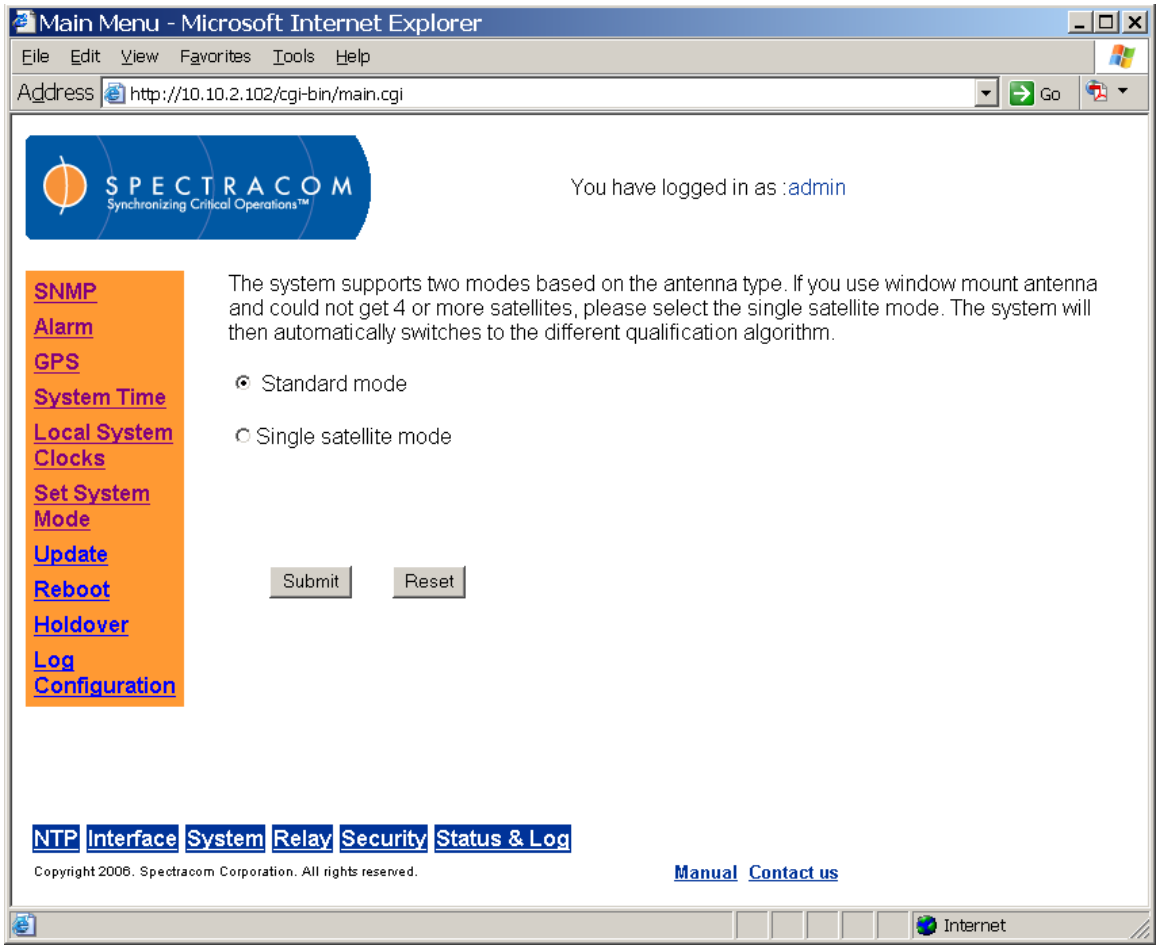

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
SNMP
Alarm
GPS
System Time
Local System Clocks
Set System Mode
Update
Reboot
Holdover
Log Configuration
The system supports two modes based on the antenna type. If you use window mount antenna and could not get 4 or more satellites, please select the single satellite mode. The system will then automatically switches to the different qualification algorithm.
Standard mode
Single satellite mode
Submit
Reset
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Internet

Figure 3-54: System Mode Screen

3.4.10 Activating System Options and Rolling Back Updates

From the System Update screen (Figure 3-55), the user may activate system options and "rollback" software updates, effectively returning the NetClock to its previous software version and configuration settings.

To activate system modem or security options, click the "Activate Option" box, choose the option you wish to activate, and enter the activation key provided by Spectracom before clicking "Submit."

To return the NetClock to its previous setup configuration ("Configuration") or software version ("Firmware"), click the appropriate selections and click "Submit."

NOTE: The NetClock must be rebooted (Figure 3-56) for the active option and configuration/firmware rollback(s) to take effect.

Figure 3-55: System Update Screen

3.4.11 Rebooting the System

The system can be rebooted from the System Reboot screen (Figure 3-56). Simply click the "Reboot Now" button and wait for the NetClock to reboot.

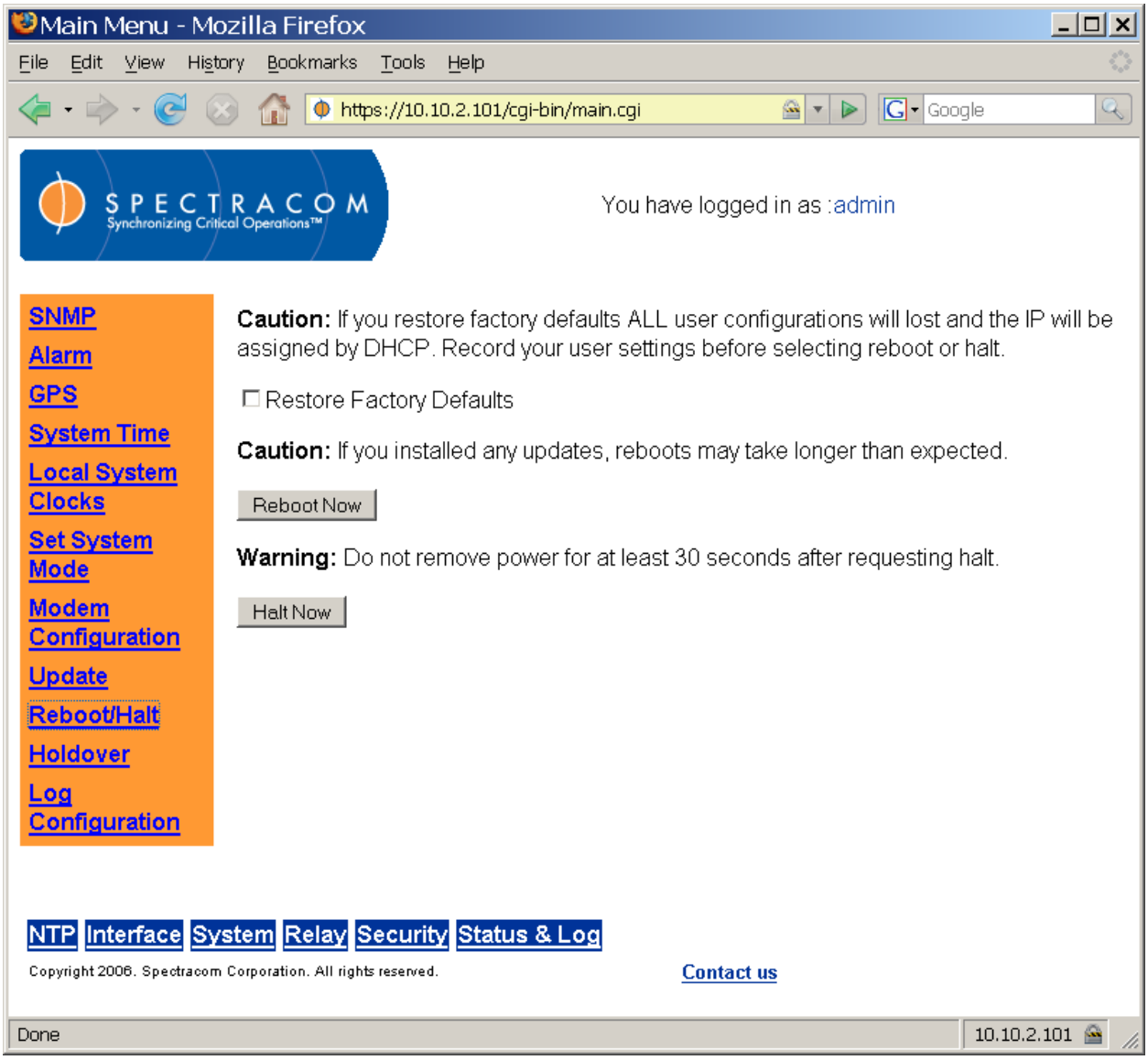

Main Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.10.2.101/cgi-bin/main.cgi
Google
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
SNMP
Alarm
GPS
System Time
Local System Clocks
Set System Mode
Modem Configuration
Update
Reboot/Halt
Holdover
Log Configuration
Caution: If you restore factory defaults ALL user configurations will lost and the IP will be assigned by DHCP. Record your user settings before selecting reboot or halt.
Restore Factory Defaults
Caution: If you installed any updates, reboots may take longer than expected.
Reboot Now
Warning: Do not remove power for at least 30 seconds after requesting halt.
Halt Now
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Done
10.10.2.101

Figure 3-56: System Reboot Screen

NOTE: If you wish to restore your NetClock to its Factory Default settings, click the checkbox labeled "Restore Factory Defaults" and then click the "Reboot Now" button. Remember that restoring the system to Factory Default settings **DOES NOT REMOVE POSITION DATA FROM THE NETCLOCK**. Refer to Section 3.4.7 for information on configuring GPS and deleting position data.

To restore the NetClock to its factory state *completely*, perform the following steps:

- Disconnect the NetClock's GPS antenna. This stops the unit from tracking satellites.

- Reset GPS from the System GPS page. (SAASM users, perform Emergency Zeroize.) This deletes the stored position in the GPS receiver and restarts the self-survey, which will commence when the GPS antenna is reattached and power is applied to the unit.
- From the System Reboot/Halt screen, select the Restore Factory Defaults option and issue the HALT command. This will shut down the Netclock. You may now remove power from the unit.
- The next unit startup, once power is applied to the unit, will take roughly 30-60 seconds longer than normal, because SSH and HTTPS keys must be regenerated.

3.4.12 Configuring System Holdover

The user may set the system holdover from the System Holdover screen (Figure 3-57). The time interval between the loss of the primary external reference and the moment that the NetClock declares loss of time synchronization is known as *holdover*. While the unit is in holdover mode, the time outputs are derived from an internal oscillator. Because of the internal oscillator, accurate time can still be derived even after the primary reference is removed. The more stable the oscillator is without an external reference, the longer this holdover period can be. The benefit of holdover is that time synchronization and the availability of the time outputs is not immediately lost when the reference is no longer available.

The NetClock has a user configurable variable holdover period so that it can be adjusted for personal requirements and desires. A user can change the length of time that a unit waits in the holdover mode before loss of time synchronization. The holdover can be defined by a specific number of hours to wait, such as 4 hours and 30 minutes. It can also be defined by the estimated error. However, the estimated error feature is only enabled for the OCXO (Option 05) and Rubidium (Option 04) products.

The estimated error rates for each oscillator are listed below. These are used when displaying the current estimated error for the user and when calculating a new holdover length (Option 04 and Option 05 oscillators only).

Oscillator	Option	Estimated Error Rates	Time to reach 2 ms
TCXO	Standard	1.0 milliseconds / hour (nominal)	2 hours (typical)
TCXO	Standard	7.2 milliseconds / hour (worst case)	17 minutes
OCXO	Option 05	72 microseconds / hour (nominal)	28 hours
Rb	Option 04	0.18 microseconds / hour (nominal)	463 days

Table 3-6: Estimated Oscillator Error Rates

NOTE: The TCXO Error rate is a worst-case estimate and not typically this value. The nominal value assumed has been 1 millisecond / hour yielding 2 hours holdover times. The OCXO and Rb oscillators use the nominal values for estimated error rate to calculate error at the end of holdover on the web browser user interface. The TCXO does not estimate error for holdover. But if it did, it probably should use the nominal value, which is more typical. Typically the error rates for a disciplined oscillator at 25 degrees Celsius will be lower than these values.

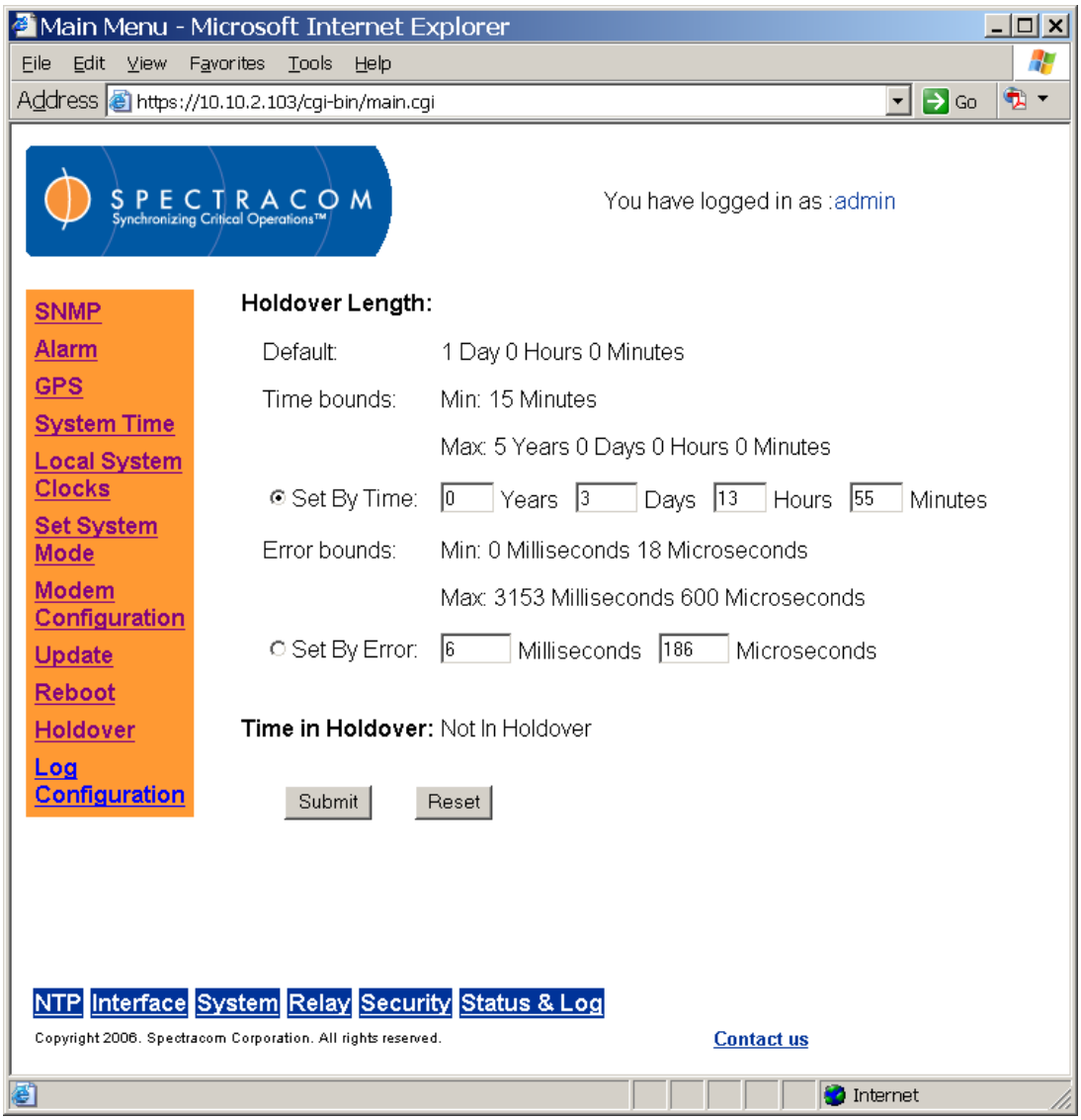


Figure 3-57: System Holdover Screen

Limits on the minimum and maximum length of allowable holdover have been placed on each oscillator as shown below in Table 3-7.

Oscillator	Minimum Length	Maximum Length
TCXO	15 minutes	24 hours
OCXO (Option 05)	15 minutes	30 days
Rb (Option 04)	15 minutes	730 days (2 years)

Table 3-7: Minimum and Maximum Allowable Holdover Values

If the user sets the length below or above the limits or if the error is too small or large, the NetClock will notify the user that this setting is outside its allowable parameters.

If the unit is currently in sync, the changes will take effect immediately. If the unit is in holdover, the changes will not take effect until the next holdover. To force the changes to take effect immediately, reboot the NetClock.

Time in Holdover displays either the amount of time that the NetClock has been in the holdover mode, or displays a phrase that the unit is not currently in the holdover mode. If the unit is currently in the holdover mode (Lost external reference but the unit is still “synchronized”), this field will show the number of days, hours, minutes and seconds that the unit has been in the holdover mode (Elapsed time from the last good external reference).

If the unit is not currently in holdover mode because it either currently receiving an external reference or because the variable holdover period has expired and the unit is no longer “synchronized”, the phrase "Not In Holdover" is displayed instead.

3.4.13 Configuring 1PPS Input

The NetClock supports an externally provided 1PPS signal, which is supplied as a reference for improved accuracy during holdover. The NetClock auto-detects this signal on the 1PPS Input connector (when provided) and uses it to maintain time only when the primary time reference (such as IRIG input) has become unstable or is no longer available. The 1PPS signal is also used between modem dial-out adjustments.

When a stable 1PPS signal is connected to the NetClock, it is recommended that the holdover timeout on the holdover setup page is adjusted to a value suitable to the desired accuracy for 1PPS source.

Oscillator	Recommended Holdover Timeout
TCXO (~2 ppm)	2 hours
OCXO (~.02 ppm)	24 hours

NOTE: Any externally provided 1pps signal should have a MINIMUM accuracy of 10ppm.

When the NetClock receives an externally-provided 1PPS input, this is indicated on the System Status page in Time Source field (Figure 3-58). Such an indication (“Ext 1PPS”) means that the NetClock has received time information from the specified time source, but is currently maintaining time using the 1PPS input signal.

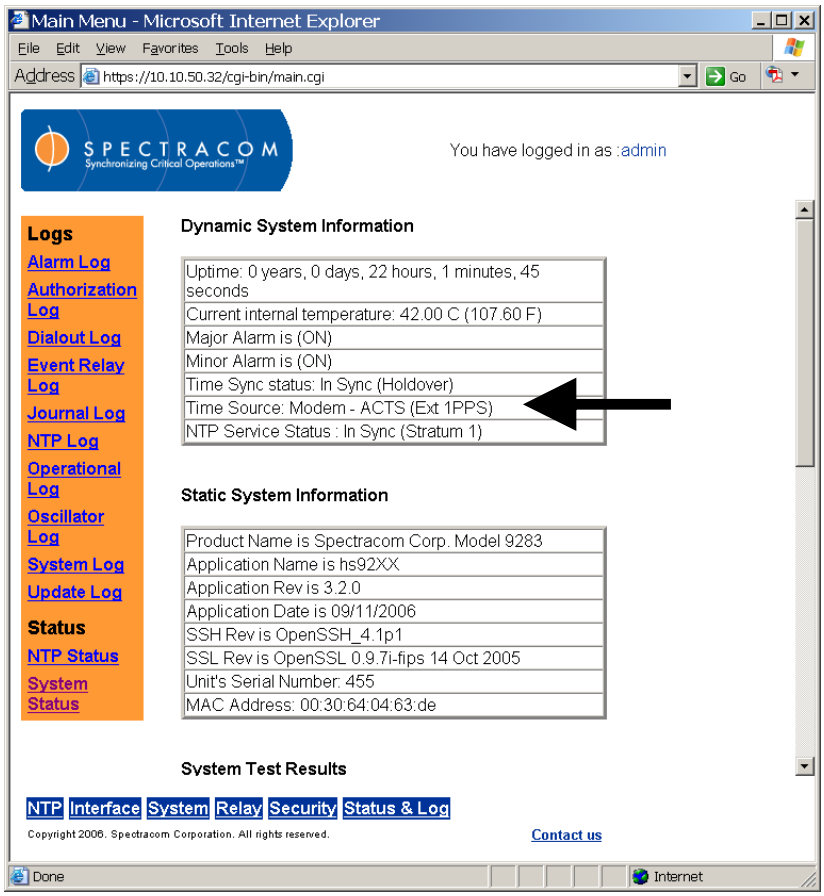


Figure 3-58: System Status Screen (1PPS Input Indicated)

3.4.14 Serial Time Code Setup

From the Serial Time Code Setup screen (Figure 3-59, 9388 models only), the user must configure the network input to be received by the Model 9388. Obtain the source output settings from your network administrator and enter the baud rate and Data Format. (The year must be entered for Data Format 0.) Click the "Submit" button when all values have been entered.

NOTE: For 9388 units ONLY, the **DATA FORMAT** must be set to match the NetClock's remote output data format. If these values do not match, the 9388 cannot synchronize. By factory default, NetClock (non-9388 time server units) output Data Format 00, while the 9388 is factory configured to receive Data Format 02. Spectracom recommends using Data Format 02, meaning the Data Format value in the NetClock must be changed from the factory default to match the factory default of the 9388.

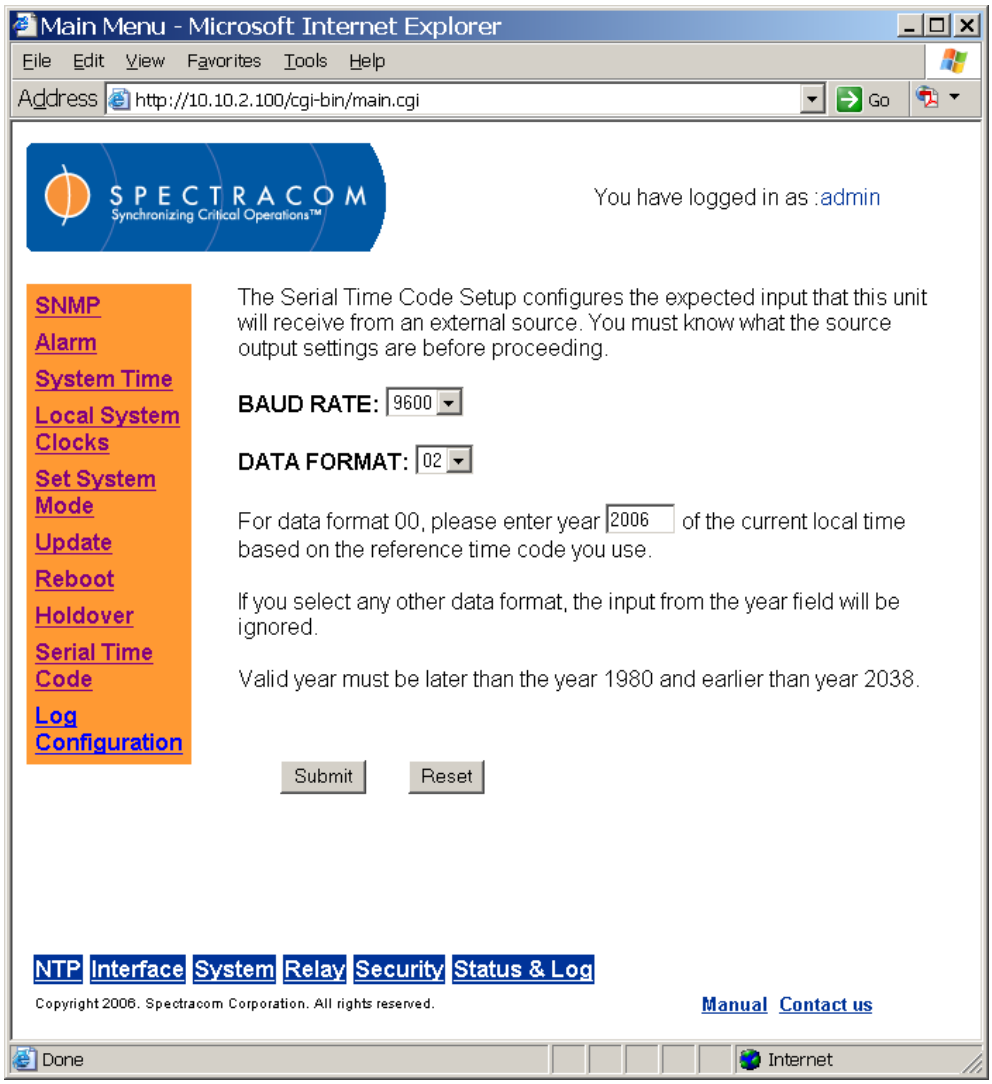

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.100/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
SNMP
Alarm
System Time
Local System Clocks
Set System Mode
Update
Reboot
Holdover
Serial Time Code
Log Configuration
The Serial Time Code Setup configures the expected input that this unit will receive from an external source. You must know what the source output settings are before proceeding.
BAUD RATE: 9600
DATA FORMAT: 02
For data format 00, please enter year 2006 of the current local time based on the reference time code you use.
If you select any other data format, the input from the year field will be ignored.
Valid year must be later than the year 1980 and earlier than year 2038.
Submit
Reset
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-59: Serial Time Code Setup Screen

NOTE: When the year is updated, the NTP server must be restarted from the NTP Web UI page (or the NetClock rebooted) for the new year value to take effect.

3.4.15 Configuring System Logs

From the System Log Configuration screen (Figure 3-60), the user may configure remote Syslog servers with which the NetClock will communicate. Facilities and severities are defined by the Syslog server and must be set up in the NetClock to match. The IP addresses and host names of the Syslog servers are entered on the bottom portion of the screen (Figure 3-61).

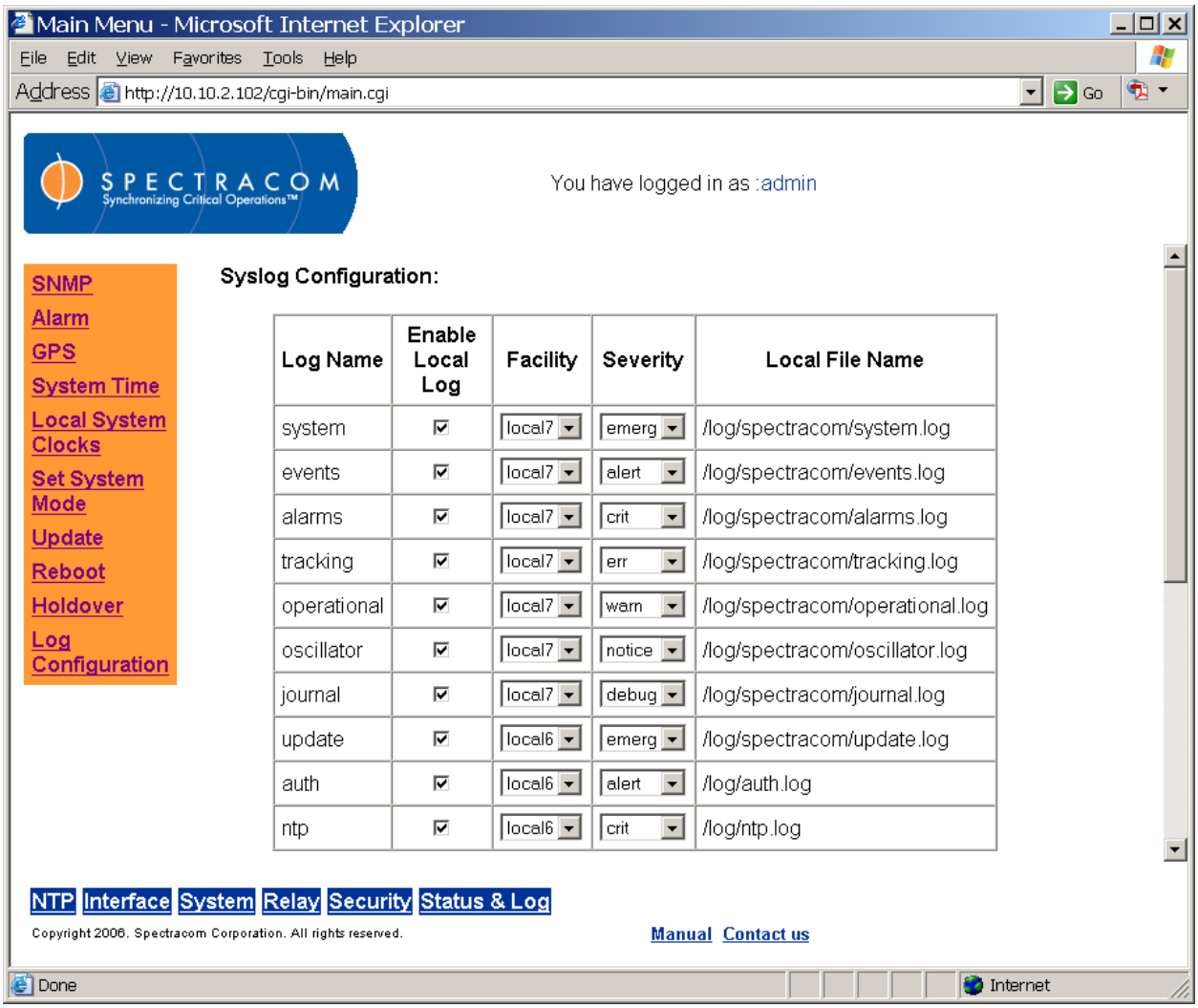

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
SNMP
Alarm
GPS
System Time
Local System Clocks
Set System Mode
Update
Reboot
Holdover
Log Configuration
Syslog Configuration:
Log Name | Enable Local Log | Facility | Severity | Local File Name
system | local7 | emerg | /log/spectracom/system.log
events | local7 | alert | /log/spectracom/events.log
alarms | local7 | crit | /log/spectracom/alarms.log
tracking | local7 | err | /log/spectracom/tracking.log
operational | local7 | warn | /log/spectracom/operational.log
oscillator | local7 | notice | /log/spectracom/oscillator.log
journal | local7 | debug | /log/spectracom/journal.log
update | local6 | emerg | /log/spectracom/update.log
auth | local6 | alert | /log/auth.log
ntp | local6 | crit | /log/ntp.log
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-60: System Log Configuration Screen (1 of 2)

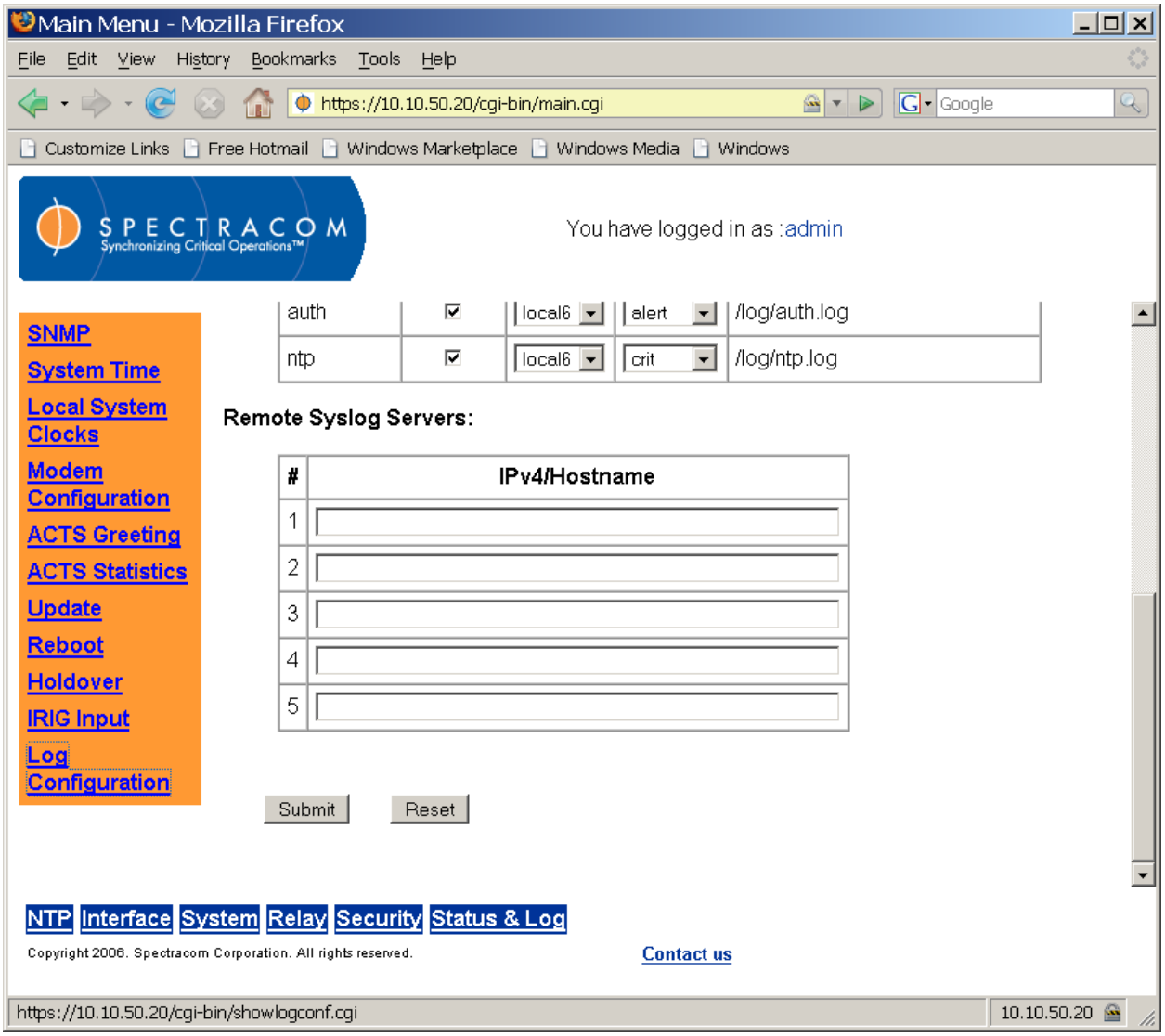


Figure 3-61: System Log Configuration Screen (2 of 2)

NOTE: Any remote syslog server that is entered to receive log messages must be properly configured to accept incoming syslog messages.

3.4.16 Configuring and Testing Relays

The Relay menu groups the NetClock's relay functions (Figure 3-62). From this menu, the user may access screens configure, test, and reset the relay outputs and event timers.

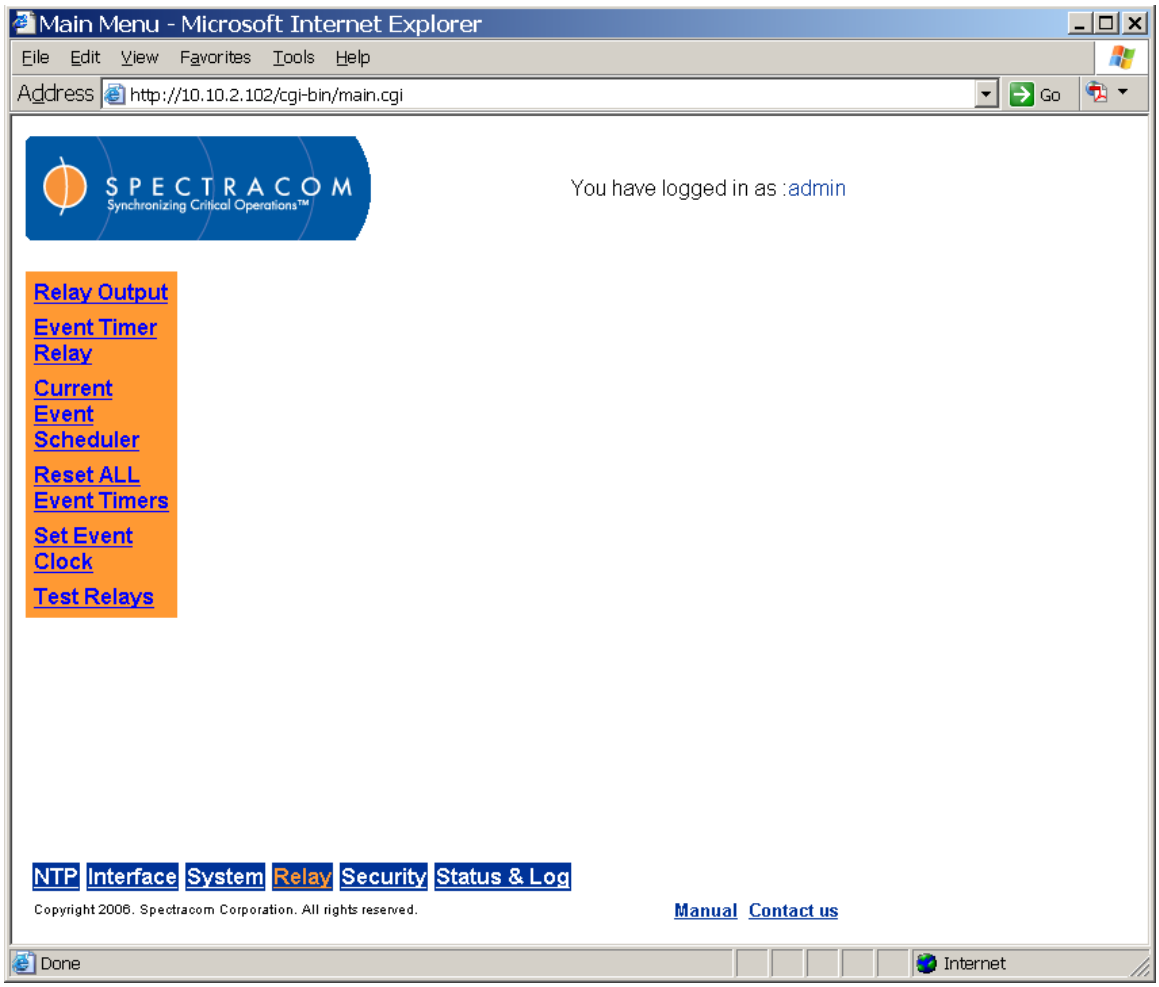


Figure 3-62: Relay Menu

The operational status can be monitored remotely using the TIMER/ALARM RELAYS connector on the rear panel. This connector provides the common, NO and NC contacts for three relays. These relays can be connected to an alarm lamp, horn, or other indicator to warn when the clock accuracy or operation has been affected, or to signal the triggering of a programmed event. The relay contacts are rated at 2.0 amps, 30VDC.

The web browser user interface allows the assignment to each relay of one of three functions: Major Alarm, Minor Alarm, and Event Timer.

To assign a function to a relay, click the radio button that lines up with both the function and the relay.The relay operation of all three relays can be tested at any time as desired. To test the relay operation, login as administrator mode and click on "test relays" in the left orange bar. Chose the desired relay to be tested and then press submit. The selected relay should activate each time the "Submit" button is pushed.

NOTE: A single relay can only be assigned one function but a function can be assigned to multiple relays. By default, all three relays are assigned “Major Alarm.”

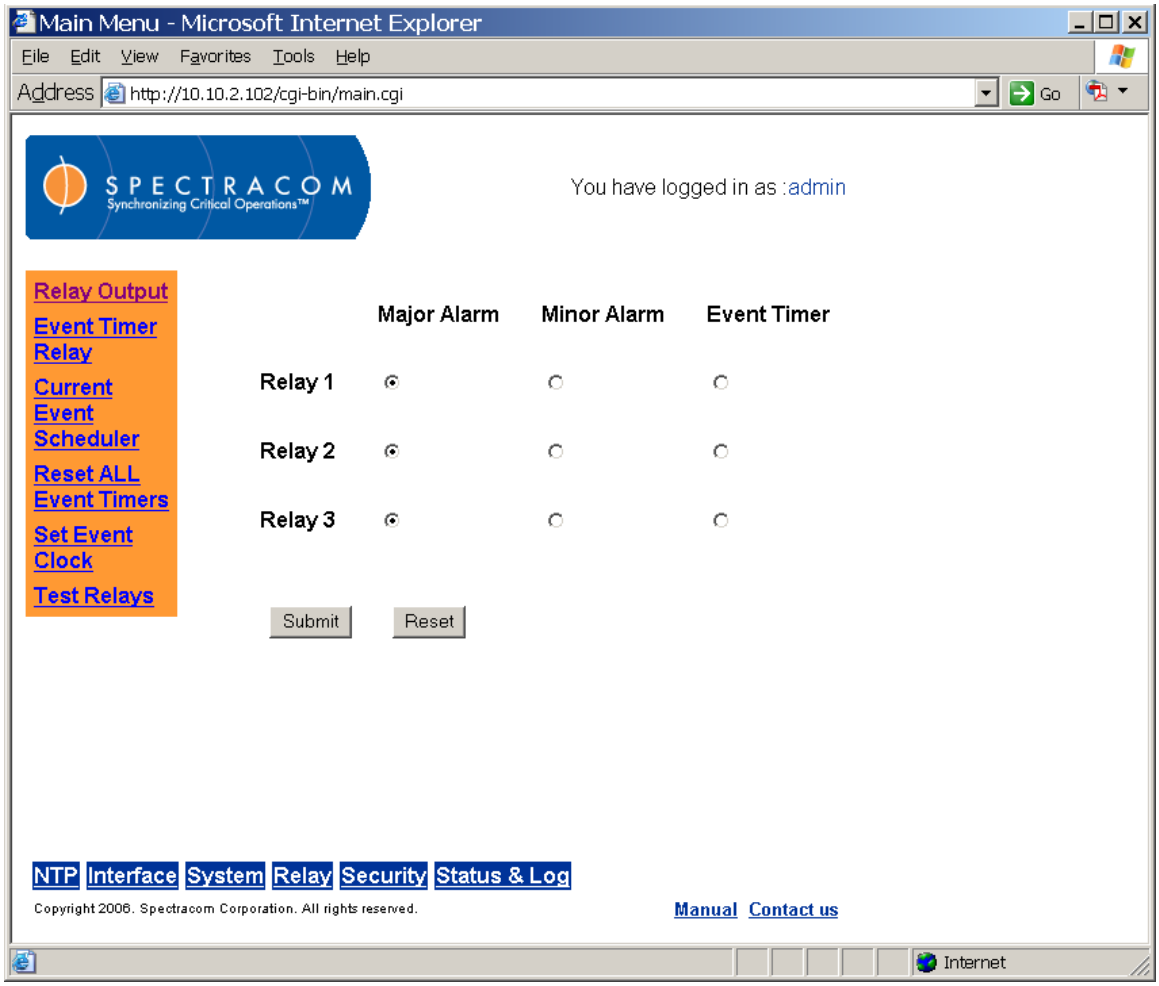


Figure 3-63: Relay Output Screen

The Event Timer Relay screen (Figure 3-64) and the Relay Current Event Scheduler screen (Figure 3-66) allow for the configuration of 128 events that can turn on or off any one of the event timer relays. Make sure the rear panel relay that is going to be associated with an event is configured to be the event timer relay in order to use this feature.

If any events are already configured, they will be displayed by event number. There are no requirements on the order of the events; each one is completely independent of the others. Enter the number of the event that you wish to edit/view and click the Edit/View button.

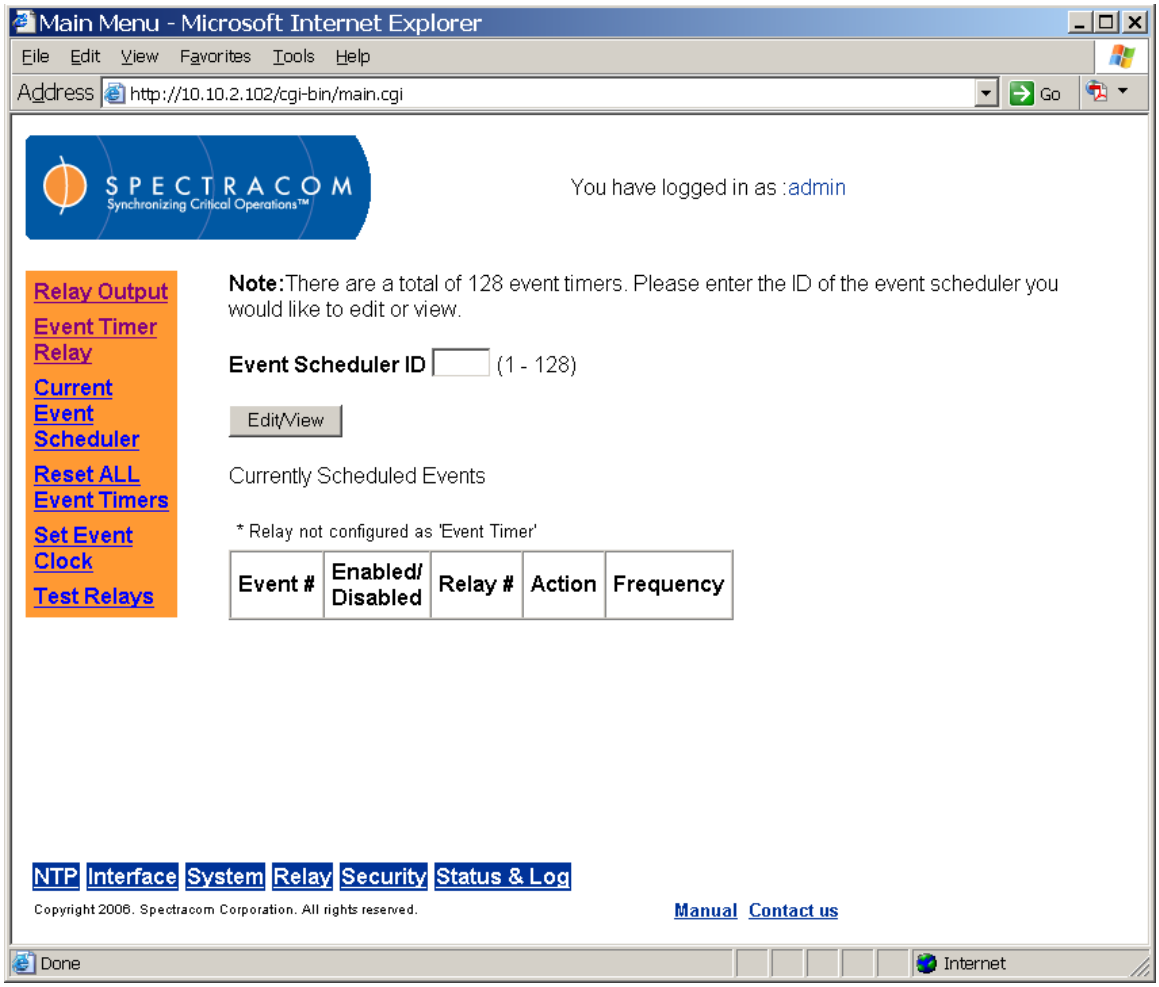

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Relay Output
Event Timer Relay
Current Event Scheduler
Reset ALL Event Timers
Set Event Clock
Test Relays
Note:There are a total of 128 event timers. Please enter the ID of the event scheduler you would like to edit or view.
Event Scheduler ID (1 - 128)
Edit/View
Currently Scheduled Events
* Relay not configured as 'Event Timer'
Event # Enabled/ Disabled Relay # Action Frequency
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-64: Event Timer Relay Screen

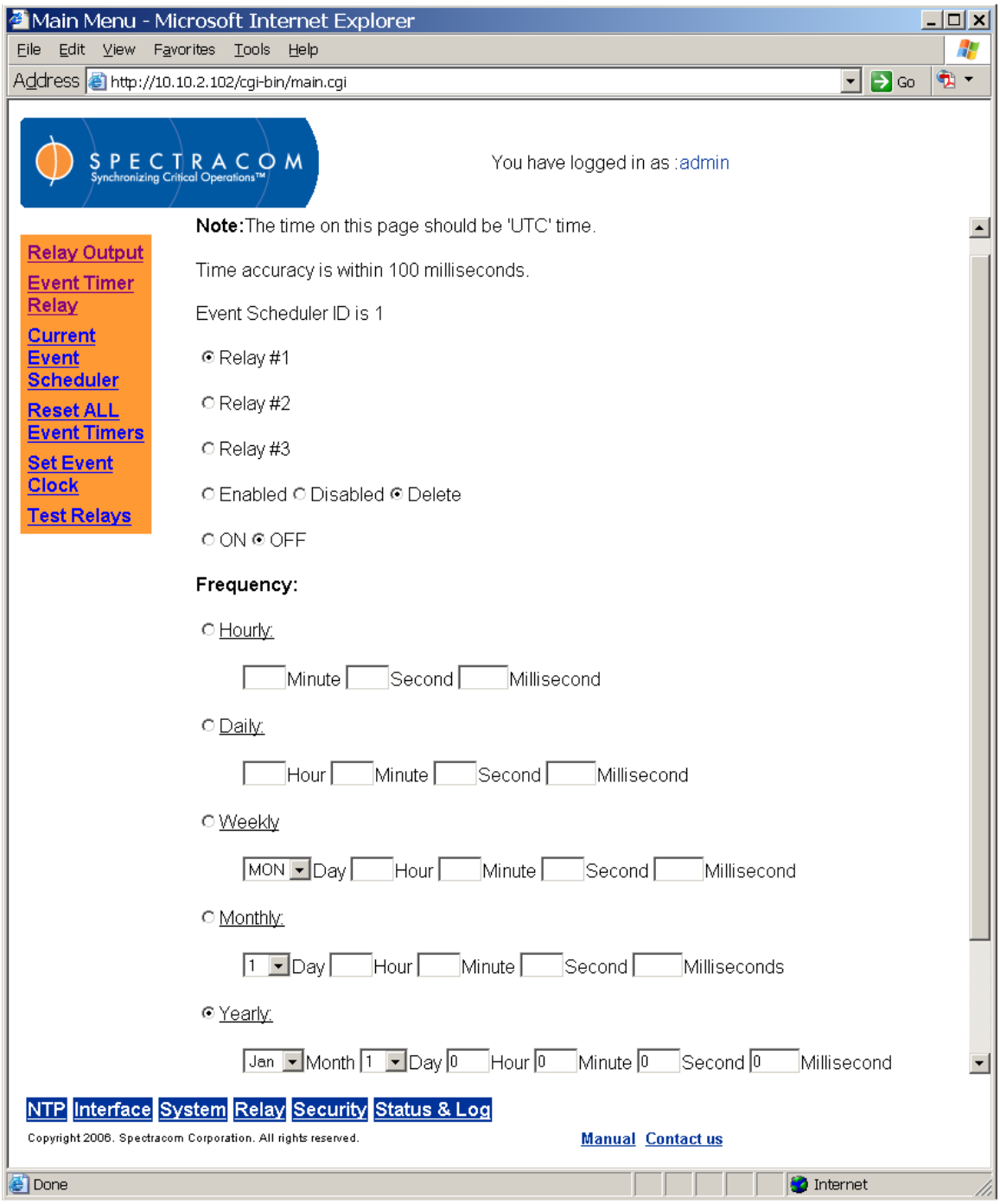


Figure 3-65: Edit/View Event Timers

Choose a Time Zone

From the left menu, select “Set Event Clock.” Choose an already defined Clock (Time Zone) or define a new one

Note: All times entered for the Event Timers will use the same Local System Clock reference for Time Zone and DST rules. It is best to choose this reference first before entering your schedule.

Relay#: Select the relay number that the event is to be associated with.

Enabled/Disabled/Delete: If the event is enabled, the event will occur when scheduled. If the event is disabled, it will not occur at the scheduled time, but will still appear in the list of scheduled events on the previous page. If the event is deleted, all fields of event are cleared and it is removed from all event lists.

ON/OFF: Each event can turn the specified event timer relay on or off.

The next section of the page describes when the event will occur and how often it will occur. The relay can be set to occur hourly, daily, weekly, monthly, and yearly.

Hourly: The event will happen every hour at the minute, second, and millisecond that is specified (within 100 milliseconds).

Daily: The event will happen every day at the hour, minute, second, and millisecond specified (within 100 milliseconds).

Weekly: The event will happen every week at the weekday, hour, minute, second, and millisecond specified (within 100 milliseconds).

Monthly: The event will happen every month at the day of month, hour, minute, second, and millisecond specified (within 100 milliseconds). If the day is set to be a day that isn't in short months, the event will happen on the last day of the short months.

Yearly: The event will happen every year at the month, day of month, hour, minute, second, and millisecond specified (within 100 milliseconds). If the month and day of month are programmed for February 29th (this can only be done while currently in a leap year), the event will happen on March 1st on non-leap years and February 29th on leap years.

NOTE: The Current Event Schedule (Figure 3-66) is a list of ENABLE events only. The events are ordered by next occurrence.

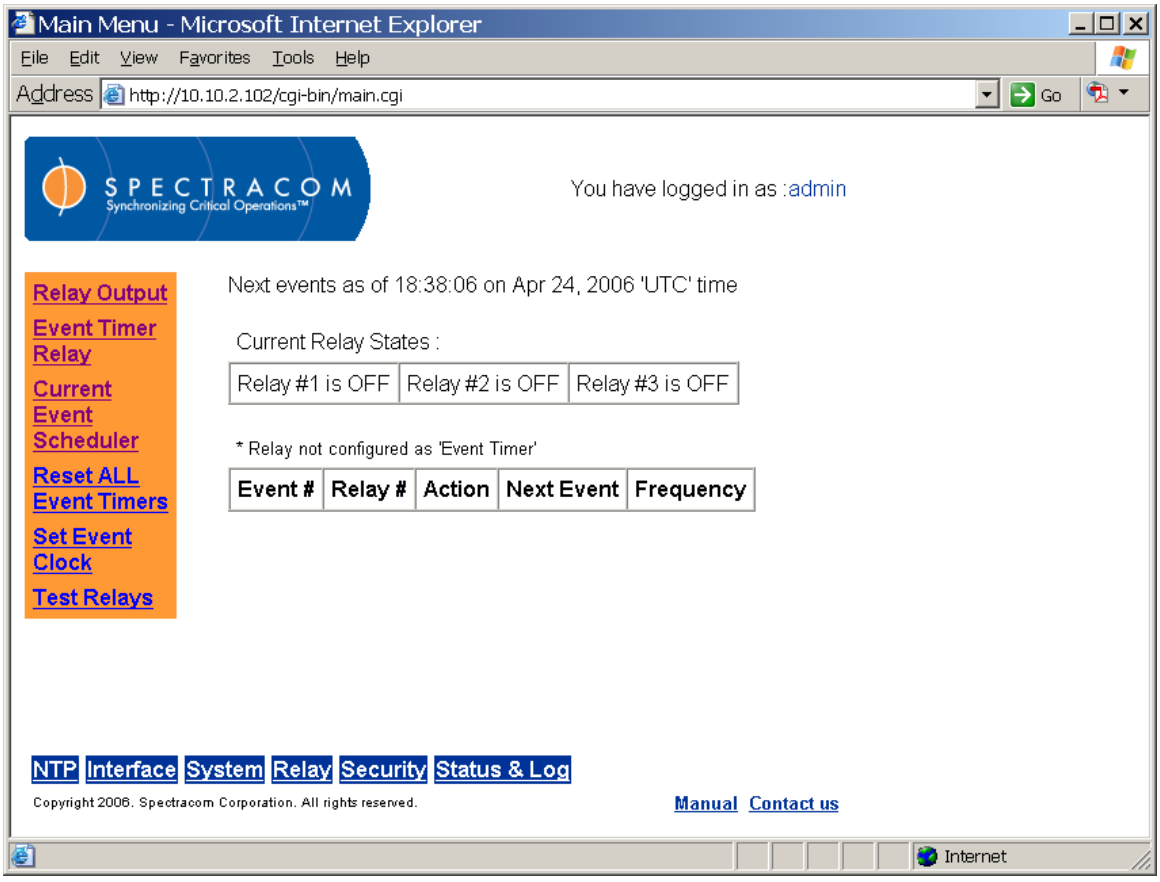

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Relay Output
Event Timer Relay
Current Event Scheduler
Reset ALL Event Timers
Set Event Clock
Test Relays
Next events as of 18:38:06 on Apr 24, 2006 'UTC' time
Current Relay States :
Relay #1 is OFF
Relay #2 is OFF
Relay #3 is OFF
* Relay not configured as 'Event Timer'
Event # Relay # Action Next Event Frequency
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Internet

Figure 3-66: Relay Current Event Scheduler Screen

From the Reset ALL Event Timers screen (Figure 3-67), the user may clear any set event timers.

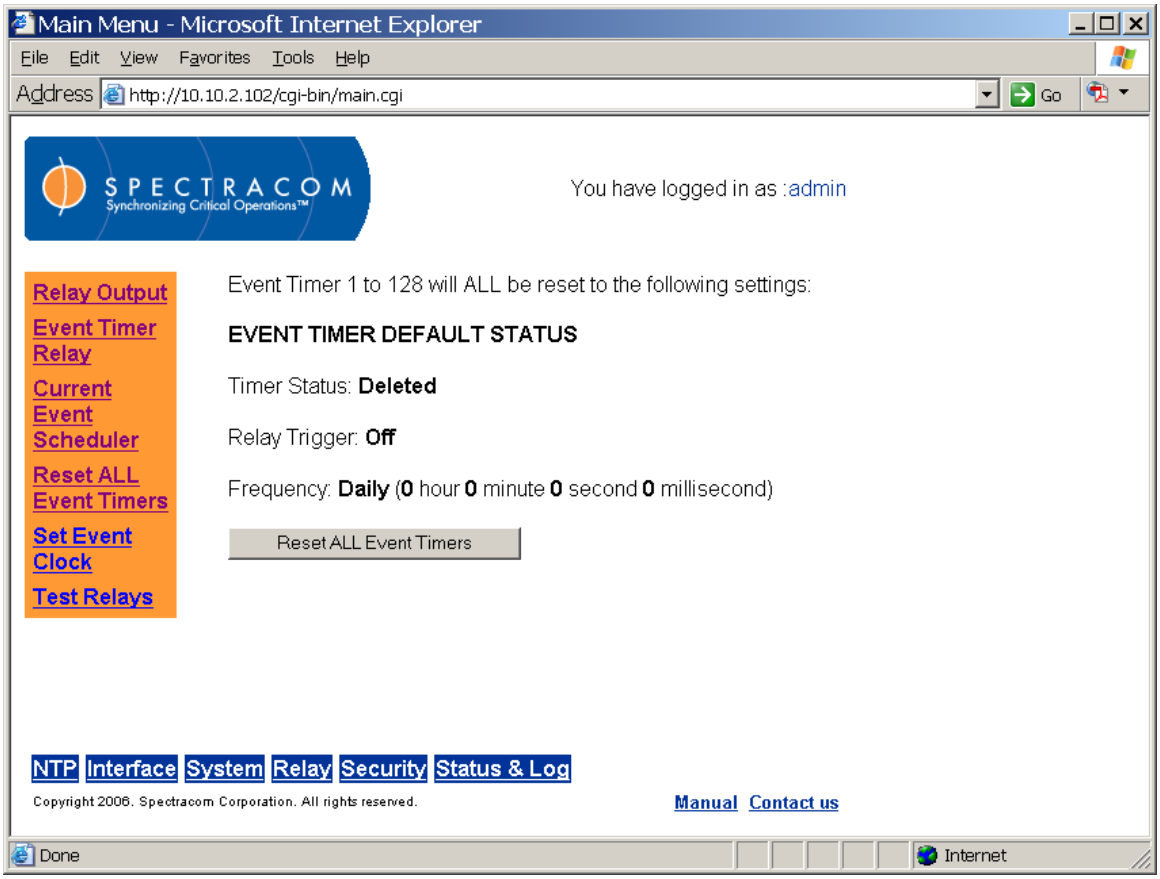

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Relay Output
Event Timer Relay
Current Event Scheduler
Reset ALL Event Timers
Set Event Clock
Test Relays
Event Timer 1 to 128 will ALL be reset to the following settings:
EVENT TIMER DEFAULT STATUS
Timer Status: Deleted
Relay Trigger: Off
Frequency: Daily (0 hour 0 minute 0 second 0 millisecond)
Reset ALL Event Timers
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-67: Relay Reset ALL Event Timers Screen

The Set Event Clock screen (Figure 3-68) allows the user to select the local system clock that drives the event function. The user may also access the create/edit local system clocks feature from this screen.

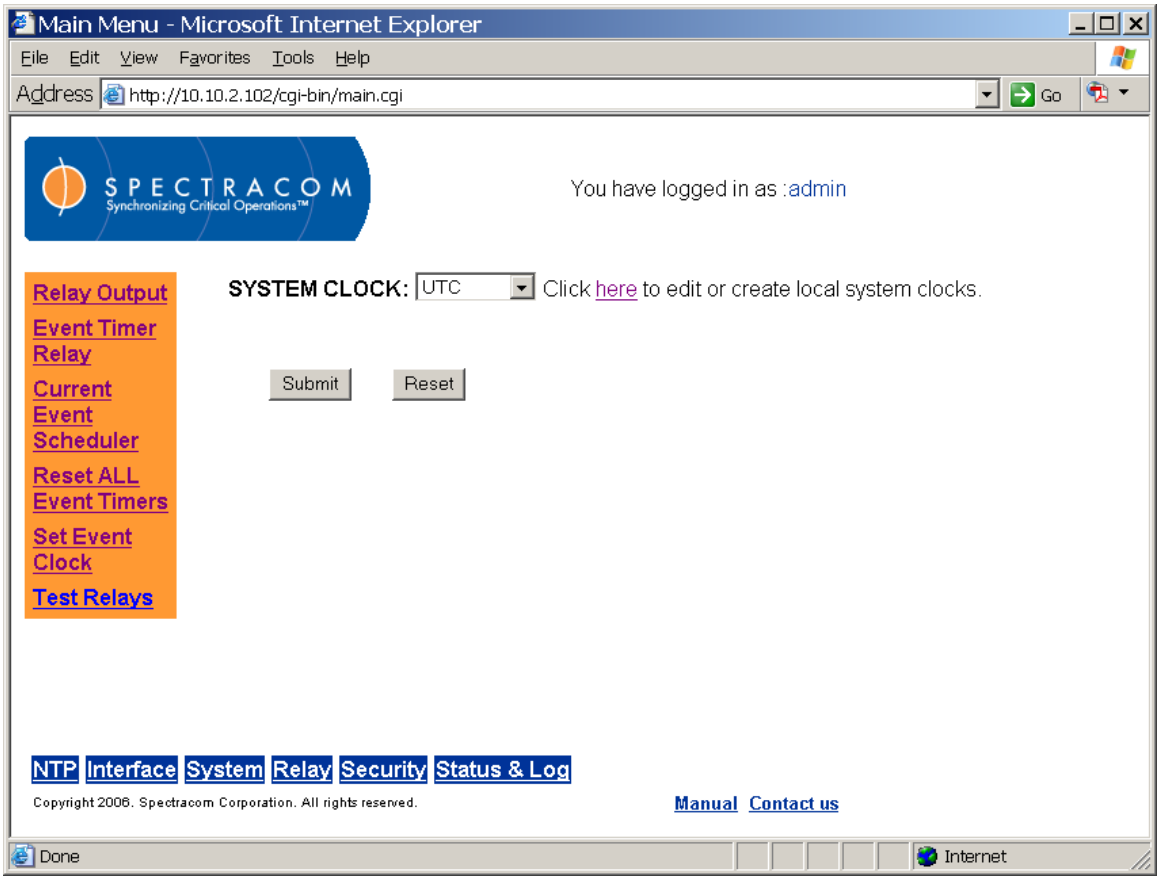


Figure 3-68: Set Event Clock Screen

Relay function can be tested from the Test Relays screen (Figure 3-69). Select one of the relays by clicking the radio button and test the selected relay by clicking Submit. If the relays are not connected to external devices, an audible clicking noise will emit from the NetClock. This noise indicates the relays are responding to the test. If external devices are connected to the relays, testing a relay should cause the connected device to actuate. When the test is complete, the Web UI will display the message, “Relay [number] test complete.”

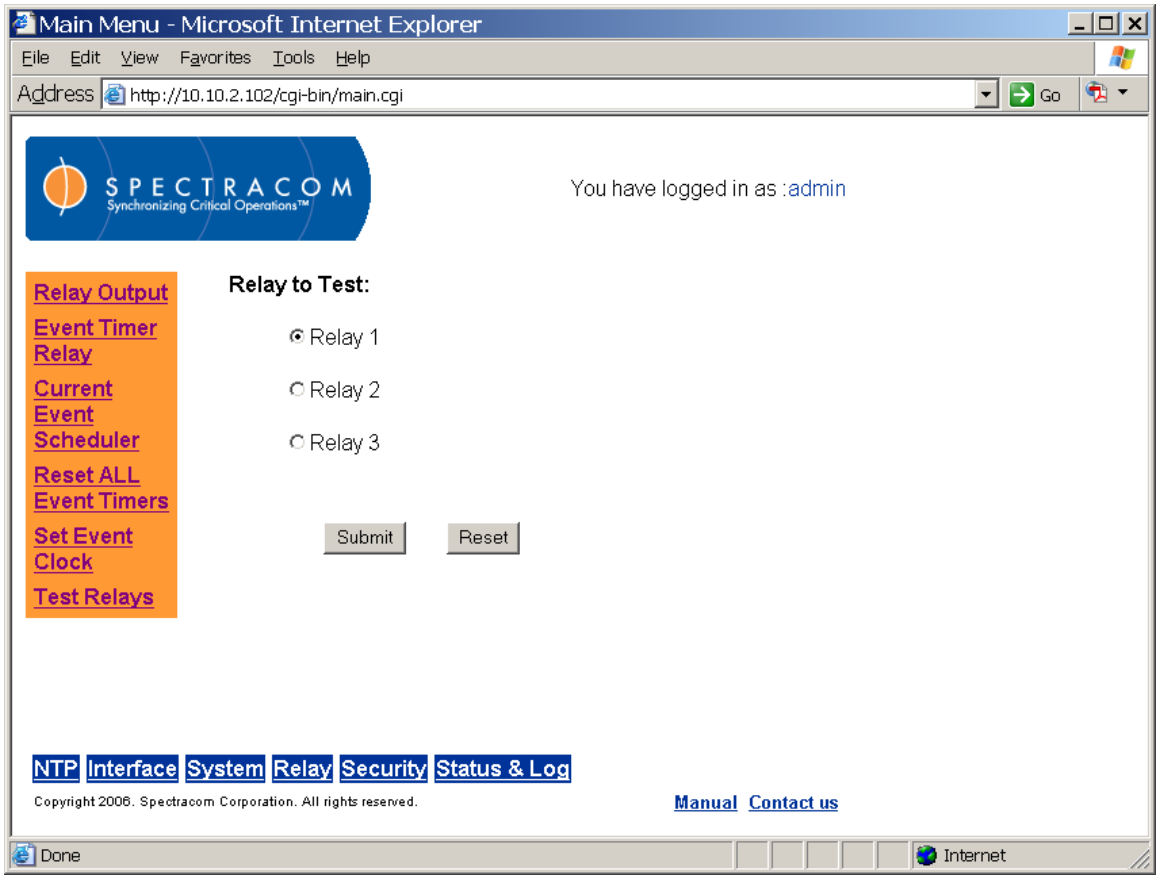


Figure 3-69: Test Relays Screen

3.4.17 Configuring Network Security

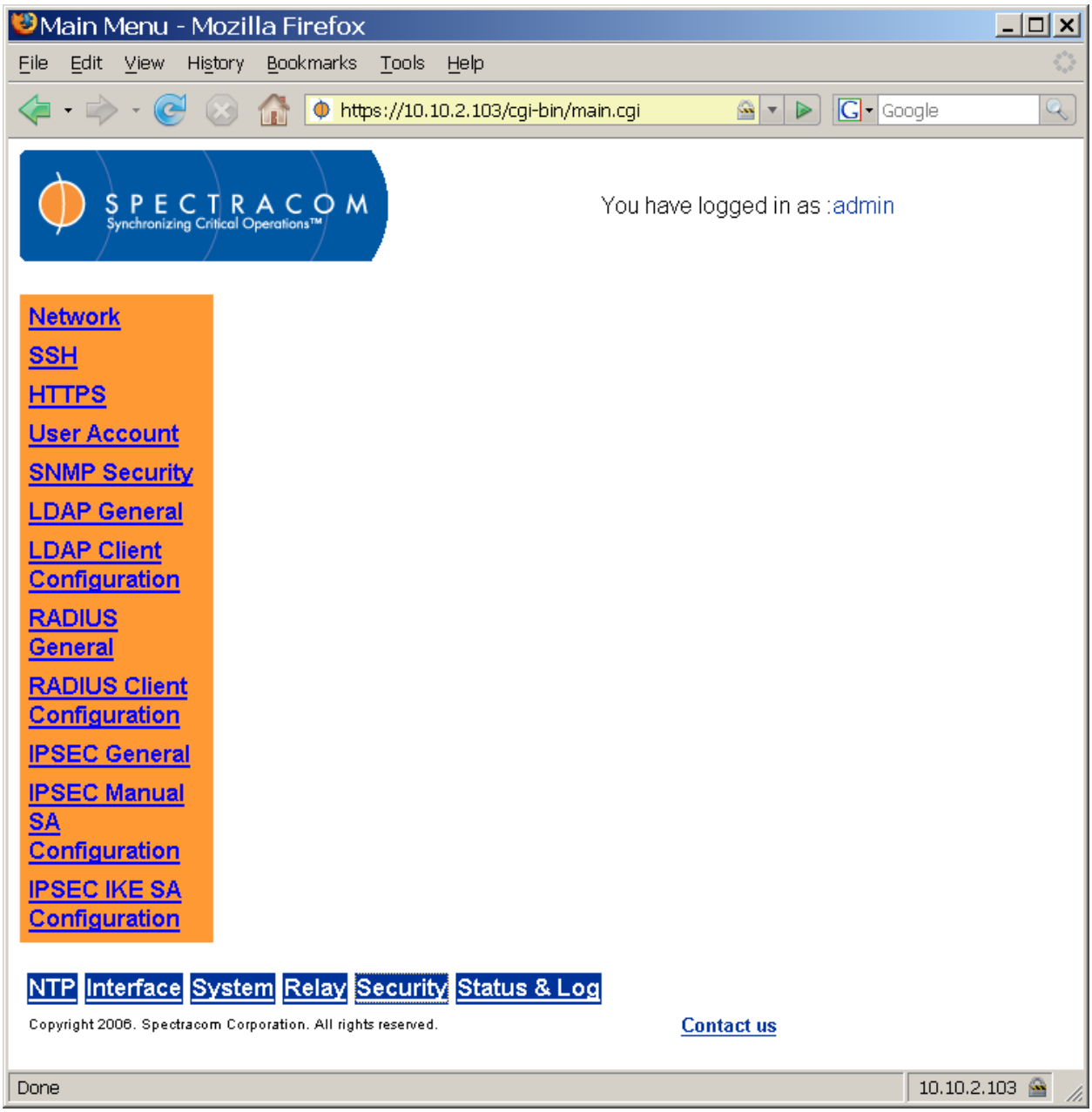


Figure 3-70: Security Menu

The Security menu groups the NetClock's security functions (Figure 3-70). From this menu, the user may access screens to configure network security, file transfers, user accounts, SNMP features, LDAP features, and RADIUS features.

Spectracom 9300 series products use OpenSSH and OpenSSL. OpenSSH is the Open Source version of the Secure Shell; which provides a set of server side tools allowing secure remote telnet like access and secure file transfer using remote copy like (RCP) and FTP like utilities.

OpenSSL is the Open Source version of Secure Sockets Library; which is used to provide the encryption libraries. Together OpenSSH and OpenSSL provide industrial strength encryption allowing for secure remote administration via command line, HTTPS web pages and secure file transfers.

The user is permitted to enable or disable HTTPS and SSH. The secure product can be configured to allow access only via NTP and the secure protocols such as HTTPS or SSH or to operate in a less secure mode.

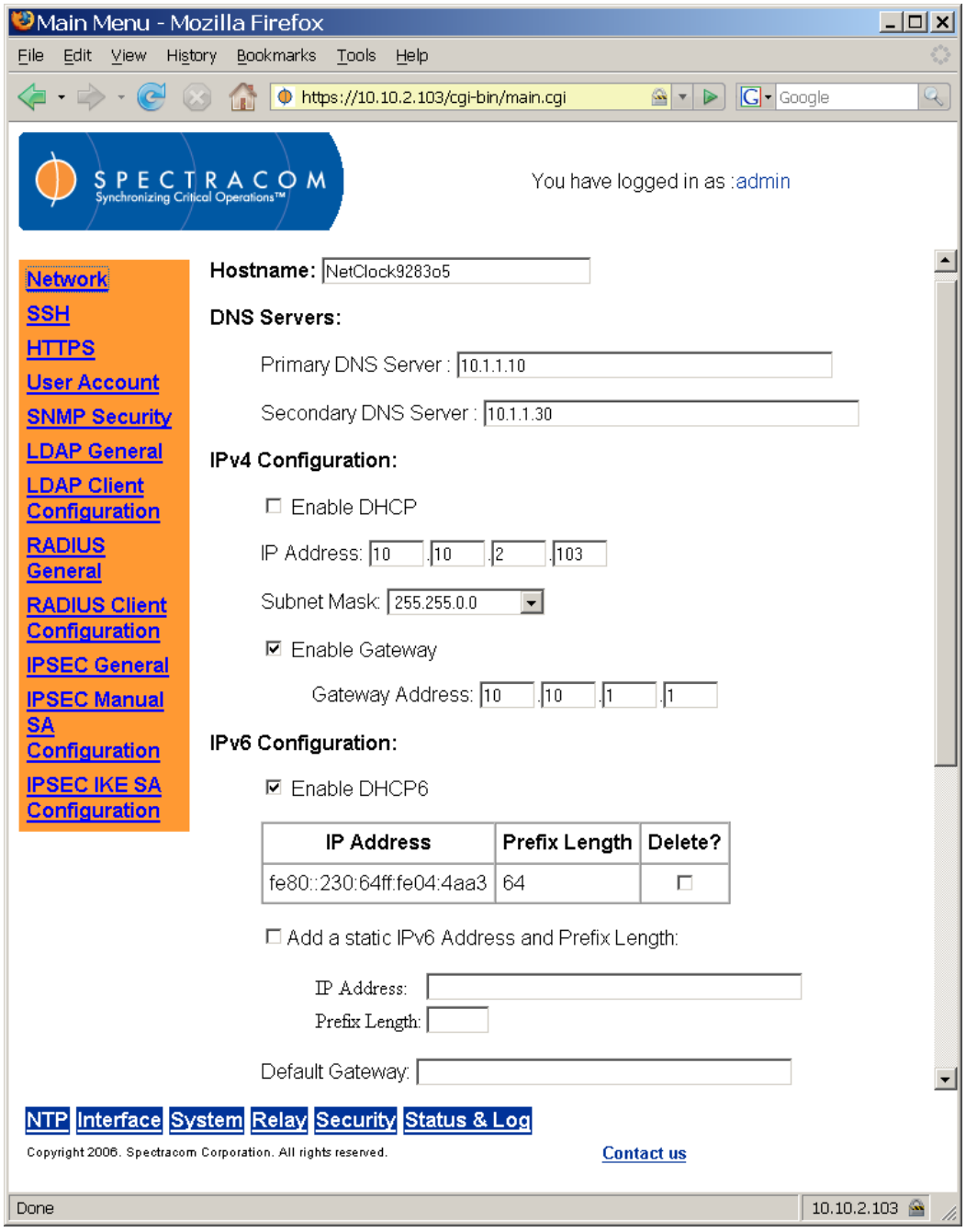


Figure 3-71: Security Network Screen (1 of 2)

From the Security Network screen (Figure 3-71), the user may define the NetClock's host name. The DNS servers are set automatically if using DHCP and manually if not using DHCP. The same is true of the IP configuration. Certain information that must be entered on this screen should be obtained from your network administrator if it is not automatically filled in.

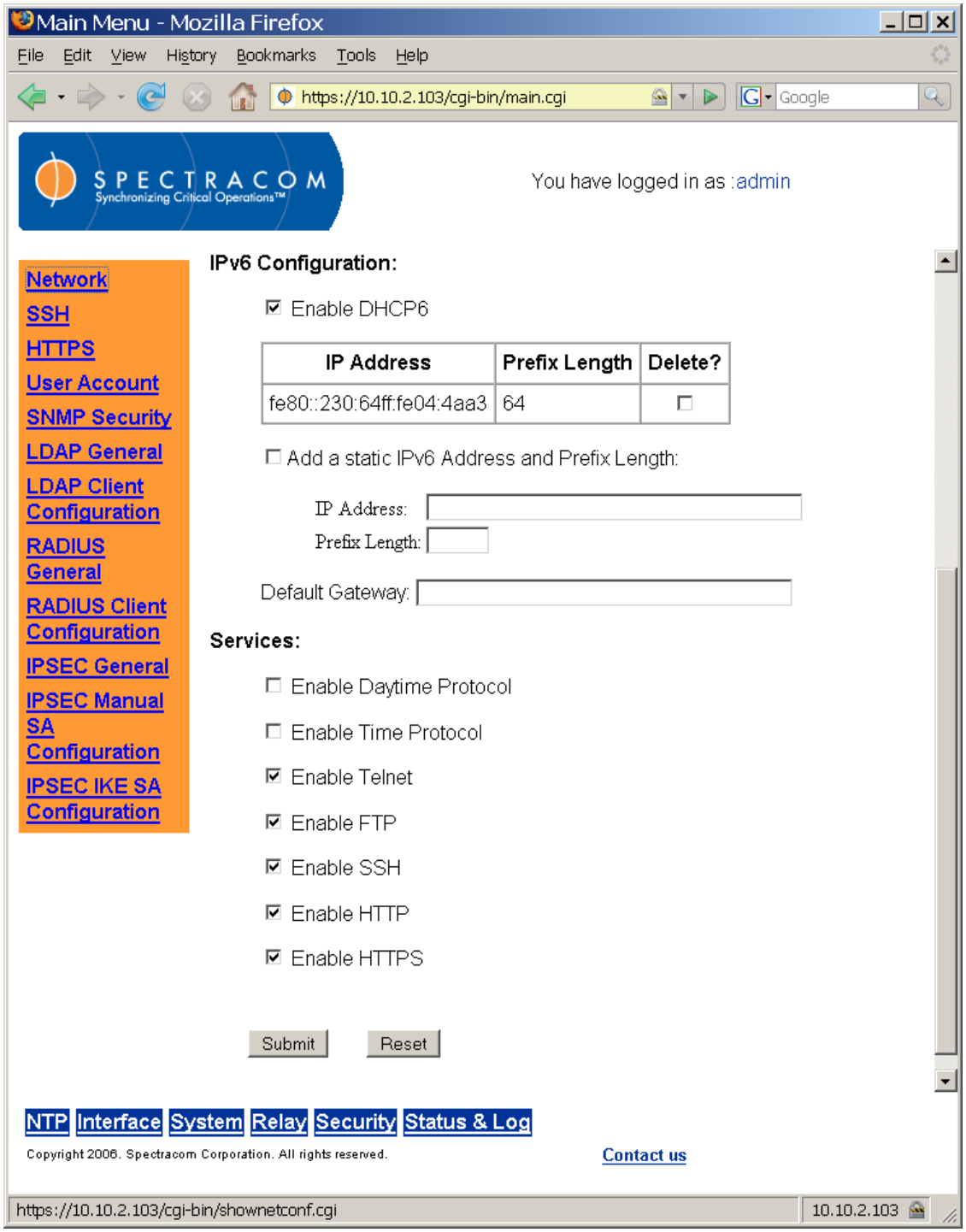


Figure 3-72: Security Network Screen (2 of 2)

3.4.17.1 Configuring SSH

SSH can be configured from the Security SSH screen (Figure 3-73). The tools supported are SSH – secure shell, SCP – secure copy, and SFTP – secure file transfer protocol. The NetClock implements the server components of SSH, SCP, and SFTP.

For more information on OpenSSH, refer to **www.openSSH.org**.

SSH uses Host Keys to uniquely identify each SSH server. Host Keys are used for server authentication and identification. The secure Spectracom product permits users to create or delete RSA or DSA keys for the SSH2 protocol.

NOTE: Due to vulnerabilities in SSH1 protocol, it is not supported. Only SSH2 is supported.

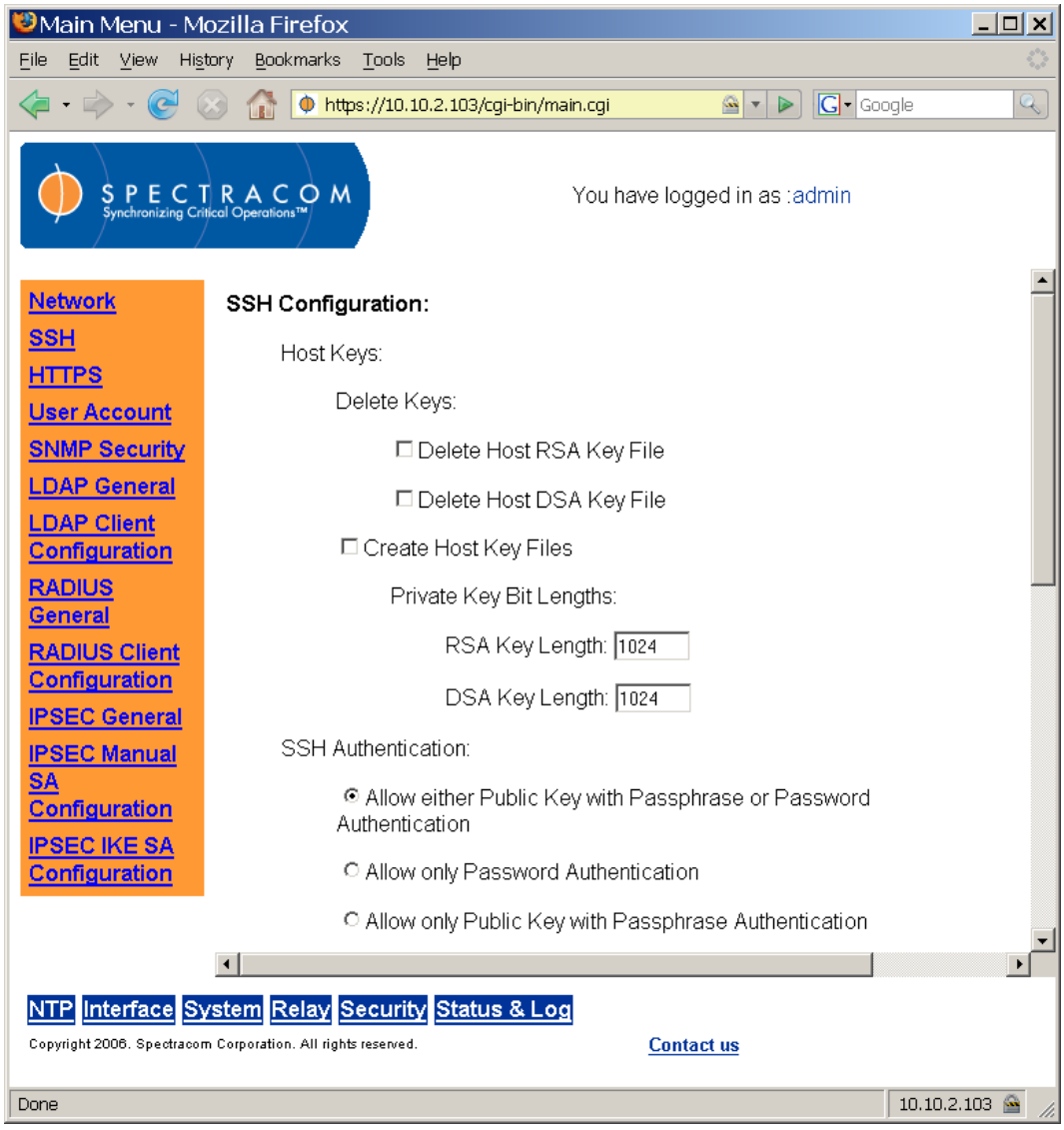


Figure 3-73: Security SSH Screen (1 of 2)

The user may choose to delete individual Host Keys. To delete a key simply select a radio button for the key you wish to delete and press submit at the bottom of the page.

If the user chooses to delete the RSA or DSA key, the SSH will function, but that form of server authentication will not be available. If the user chooses to delete both the RSA and DSA keys, SSH will not function. In addition, if SSH Host Keys are being generated at the time of deletion, the key generation processes are stopped, any keys created will be deleted, and all key bit sizes are set to 0.

The user may choose to delete existing keys and request the creation of new keys, but it is often simpler to make these requests separately.

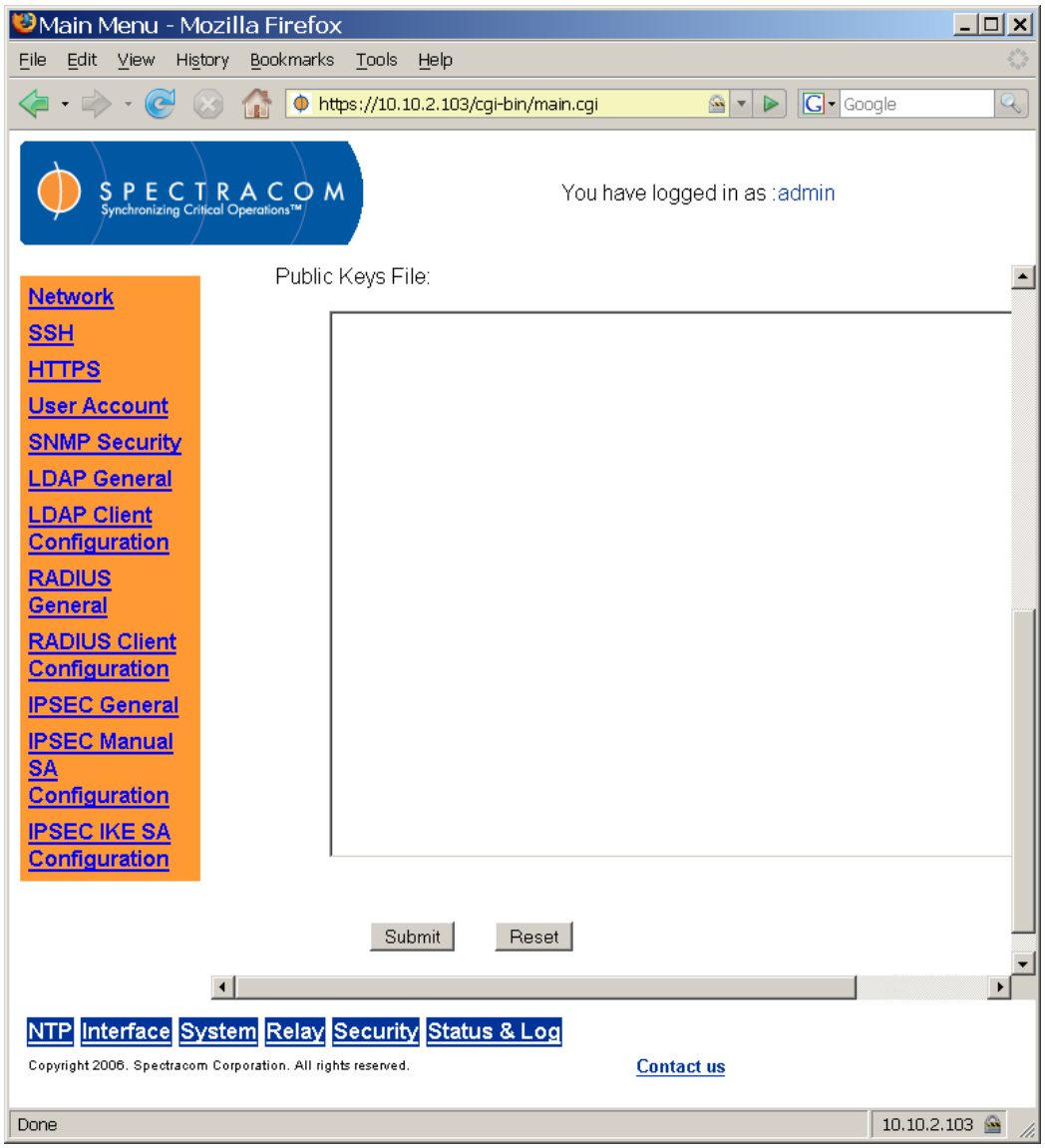


Figure 3-74: Security SSH Screen (2 of 2)

The user may create individual RSA and DSA Host Public/Private Key pairs. Host Keys must first be deleted before new Host Keys can be created. To create a new set of host keys first

delete the old keys, then select the create host keys checkbox and enter the key sizes you desire. Then select the “Submit” button at the bottom of the screen.

Spectracom secure products typically have their initial Host Keys created at the factory. The default key size for all key types is 1024. Host Key sizes can vary between 768 and 4096 bits. The recommended key size is 1024. Though many key sizes are supported, it is recommended that users select key sizes that are powers of 2 or divisible by 2. The most popular sizes are 768, 1024, and 2048. Large key sizes up to 4096 are supported, but may take ten minutes or more to generate.

Host Keys are generated in the background. Creating RSA and DSA keys, each with 1024 bits length, typically takes about 30 seconds. Keys are created in the order of RSA, DSA and finally RSA1. When the keys are created you can successfully make SSH client connections. If the unit is rebooted with Host Key creation in progress or the unit is booted and no host keys exist the key generation process is restarted. The key generation process uses either the previously specified key sizes or if a key size is undefined it defaults to 1024. A key with a zero length or blank key size field is not created.

Note also that when you delete a Host Key and recreate a new one, SSH client sessions will warn you that the host key has changed for this particular IP address. The user will either have to override the warning and accept the new Public Host Key and start a new connection or they may need to remove the old Host Public Key from their client system and accept the new Host Public Key. Please consult your specific SSH client’s software’s documentation.

The SSH client utilities SSH, SCP, and SFTP allow for several modes of user authentication. SSH allows the user to remotely login or transfer files by identifying the user’s account and the target machines IP address. Users can be authenticated by either using their account passwords or by using a Public Private Key Pair. Users keep their private key secret within their workstations or network user accounts and provide the NetClock a copy of their public key. The modes of authentication supported include:

- Either Public Key with Passphrase or Login Account Password
- Login Account Password only
- Public Key with Passphrase only

The first option allows users to login using either method. This is the default. Whichever mode works is allowed for logging in. If the Public Key is not correct or the Passphrase is not valid the user is then prompted for the login account password. The second option simply skips public/private key authentication and immediately prompts the user for password over a secure encrypted session avoiding sending passwords in the clear. Finally the last option requires the user to load a public key into the NetClock. This public key must match the private key found in the users account and be accessible to the SSH, SCP, or SFTP client program. The user must then enter the Passphrase after authentication of the keys to provide the second factor for 2-factor authentication.

SSH using public/private key authentication is the most secure method of authenticating users for SSH, SCP or SFTP sessions.

The web browser user interface provides the means for the user to view and edit the authorized_keys file, to add Public Keys. Using FTP, SCP, or SFTP the user may also retrieve the authorized_keys file from the.ssh directory.

An example of a user adding a public key to the authorized_keys file is shown below.

Users are required to create private and public key pairs on their workstation or within a private area in their network account. These keys may be RSA or DSA and may be any key bit length as supported by the SSH client tool. These public keys are stored in a file in the .ssh directory named authorized_keys. The file is to be formatted such that the key is followed by the optional comment with only one key per line. The file format, line terminations, and other EOL or EOF characters should correspond to UNIX conventions, not Windows.

If a user deletes all Public Keys Public/Private Key Authentication is disabled. If the user has selected SSH authentication using the “Public Key with Passphrase” option login and file transfers will be forbidden. The user must select a method allowing the use of account password authentication to enable login or file transfers using SCP or SFTP.
If a user wants to completely control the public keys used for authentication, a correctly formatted authorized_keys file formatted as indicated in the OpenSSH web site can be loaded onto a secure Spectracom product. The user transfers a new public key file using an insecure FTP client or a secure SCP or SFTP client using only account password authentication. The user should place the new public key’s file in the .ssh directory.

Secure shell sessions using an SSH client can be performed using the admin or a user-defined account. The user may use Account Password or Public Key with Passphrase authentication. The OpenSSH tool SSH-KEYGEN may be used to create RSA and DSA keys used to identify and authenticate user login or file transfers.

The following command lines for OpenSSH SSH client tool are given as examples of how to create an SSH session.

Creating an SSH session with Password Authentication for the admin account:
ssh admin@10.10.200.5
admin@10.10.200.5's password: admin123

The user is now presented with Boot up text and/or a “>” prompt which allows the use of the Spectracom command line interface.

Creating an SSH session using Public Key with Passphrase Authentication for the admin account:

The user must first provide the secure Spectracom product a RSA public key found typically in the OpenSSH id_rsa.pub file. The user may then attempt to create an SSH session.

ssh -i ./id_rsa admin@10.10.200.5
Enter passphrase for key './id_rsa': mysecretpassphrase

Please consult the SSH client tool’s documentation for specifics on how to use the tool, select SSH protocols, and provide user private keys.

3.4.17.2 Secure File Transfer

NetClocks provide secure file transfer using the SSH client tools SCP and SFTP. Authentication is performed using either Account Passwords or Public Key with Passphrase. However, unlike SSH, in which the admin or a user-defined account is used, a special user account is provided

named “SCP” for these tools. The “SCP” user account has the same password as the admin account. It differs from the admin account in that it does not run the Spectracom product shell. It is a limited account that only allows the user to transfer files to and from the product file system folder and to retrieve files from folders which the SCP account has read permission.

Some sample OpenSSH, SCP, and SFTP client commands are shown below.

1) Perform an SCP file transfer to the device using Account Password authentication

scp authorized_keys scp@10.10.200.5:.ssh
scp@10.10.200.135's password: admin123 (Always use same password as admin)

publickeys 100% |**********| 5 00:00

2) Perform an SCP file transfer from the device using Public Key with Passphrase authentication.

scp -i ./id_rsa scp@10.10.200.5:.ssh
Enter passphrase for key './id_rsa': mysecretpassphrase

publickeys 100% |**********| 5 00:00

3) Perform an SFTP file transfer to the device using Account Password authentication.

sftp scp@10.10.200.5
scp@10.10.200.135's password: admin123 (Always use same password as admin)

sftp>

The user is presented with the SFTP prompt allowing interactive file transfer and directory navigation.

4) Perform an SFTP file transfer from the device using Public Key with Passphrase authentication

sftp -i ./id_rsa scp@10.10.200.5
Enter passphrase for key './id_rsa': mysecretpassphrase

sftp>

The user is presented with the SFTP prompt allowing interactive file transfer and directory navigation.

NOTE: Use of SCP and SFTP is restricted to the administrator. To access SCP, enter the account name SCP with your administrator password. For SFTP, the account name is SCP.

3.4.17.3 Recommended SSH Client Tools

Spectracom does not make specific recommendations as to which specific SSH client, SCP client, or SFTP client tools. However, there are many SSH based tools available at cost or free to the user.

Two good, free examples of SSH tool suites are the command line based OpenSSH running on a Linux or OpenBSD x86 platform and the excellent (and free) putty SSH tool suite.

The OpenSSH tool suite in source code form is freely available at www.openSSH.org though you must also provide an OpenSSL library, which can be found at www.openssl.org.

The putty SSH tools and instructions regarding their use can be found at:
HTTP://www.chiark.greenend.org.uk/~sgtatham/putty/

3.4.17.4 Configuring HTTPS

The OpenSSL library provides the encryption algorithms used for secure HTTP (HTTPS) (Figure 3-75). The OpenSSL package also provides tools and software, which is used to create x509 Certificate Requests, Self Signed Certificates and Private/Public Keys. The NetClock uses OpenSSL library with a simple GUI interface to create certificate Requests and self-signed certificates. Users can then send these certificate requests to an external Certificate Authority (CA) for the creation of a third party verifiable certificate or use an internal corporate CA. If a Certificate Authority is not available the user can simply use the self-signed certificate that comes with the unit until it expires or create their own self-signed certificates to allow the use of HTTPS.

NOTE: If the IP Address or Common Name (Host Name) is changed, you may wish to regenerate the security certificate. Otherwise you may receive security warnings from your web browser.

Each Spectracom secure product comes with a default Spectracom self-signed certificate, which will outlast the product warranty. The typical expiration of the certificate is about 10 years. HTTPS is available using this certificate until this certificate expires. If deleted however, this certificate cannot be restored.

For more information on OpenSSL please see www.openssl.org.

The NetClock's software supports x509 DER and PEM and P7 PKCS#7 PEM and DER formatted certificates. The user can create a customer specific x509 self-signed certificate, an RSA private key and x509 certificate request using the web browser user interface. RSA private keys are supported because they are the most widely accepted. (At this time, DSA keys are not supported.)

3.4.17.5 Requesting Certificate Authority Certificates

Once the processing to create the certificate request, RSA private key, and self-signed certificate is completed, the Web UI will display the certificate request.

The user can submit this certificate request to the company's Certificate Authority for a verifiable, authenticable third party certificate. Until this certificate is received, the user's self-signed certificate, displaying the information shown herein, can be used.

The NetClock will load this new self-signed certificate and private key after the user selects a few more web page options or when the user selects the “Exit connection to product” button at the top of the screen. You will see a pop up window in Windows operating systems. The certificate can be installed or viewed using this pop up window. Other operating systems may vary in how they install and accept certificates. External Internet access may be required by your Certificate Authority to verify your third party certificate.

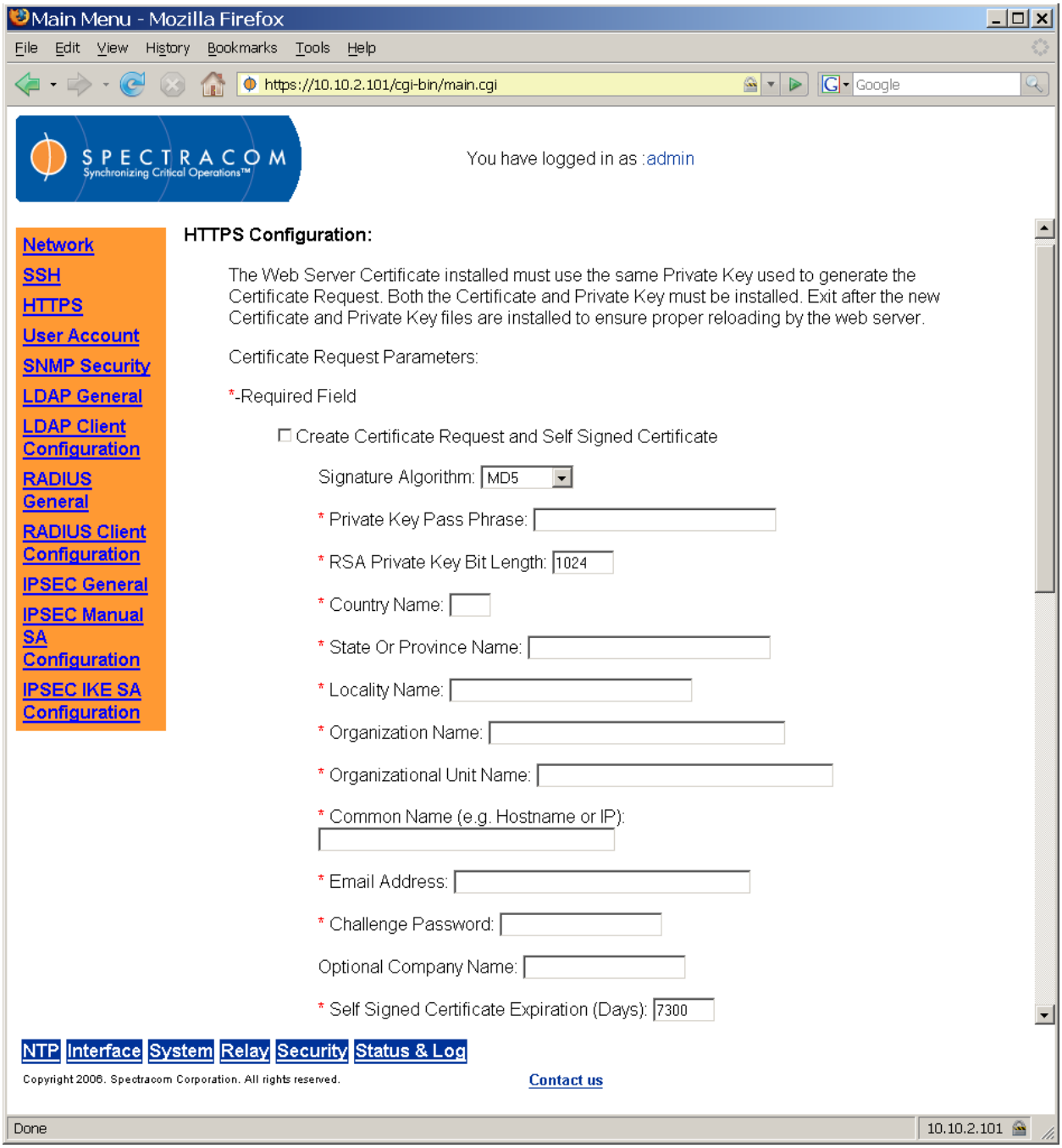

Main Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.10.2.101/cgi-bin/main.cgi
Google
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Network
SSH
HTTPS
User Account
SNMP Security
LDAP General
LDAP Client Configuration
RADIUS General
RADIUS Client Configuration
IPSEC General
IPSEC Manual SA Configuration
IPSEC IKE SA Configuration
HTTPS Configuration:
The Web Server Certificate installed must use the same Private Key used to generate the Certificate Request. Both the Certificate and Private Key must be installed. Exit after the new Certificate and Private Key files are installed to ensure proper reloading by the web server.
Certificate Request Parameters:
*-Required Field
Create Certificate Request and Self Signed Certificate
Signature Algorithm: MD5
* Private Key Pass Phrase:
* RSA Private Key Bit Length: 1024
* Country Name:
* State Or Province Name:
* Locality Name:
* Organization Name:
* Organizational Unit Name:
* Common Name (e.g. Hostname or IP):
* Email Address:
* Challenge Password:
Optional Company Name:
* Self Signed Certificate Expiration (Days): 7300
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Done
10.10.2.101

Figure 3-75: Security HTTPS Screen (1 of 2)

3.4.17.5.1 Updating x509 PEM Certificate Files using the Web UI

The user is required to select a signature algorithm, a private key passphrase of at least 4 characters, a private key bit length, the certificates expiration in days and at least one of the remaining fields. It is recommended that the user consult their Certificate Authority for the required fields in an x509 certificate request. Spectracom recommends all fields be filled out and match the information given to your certificate authority. For example, use all abbreviations, spellings, URLs, and company departments recognized by the Certificate Authority. This helps in avoiding issues with the Certificate Authority having issues to reconciling certificate request and company record information.

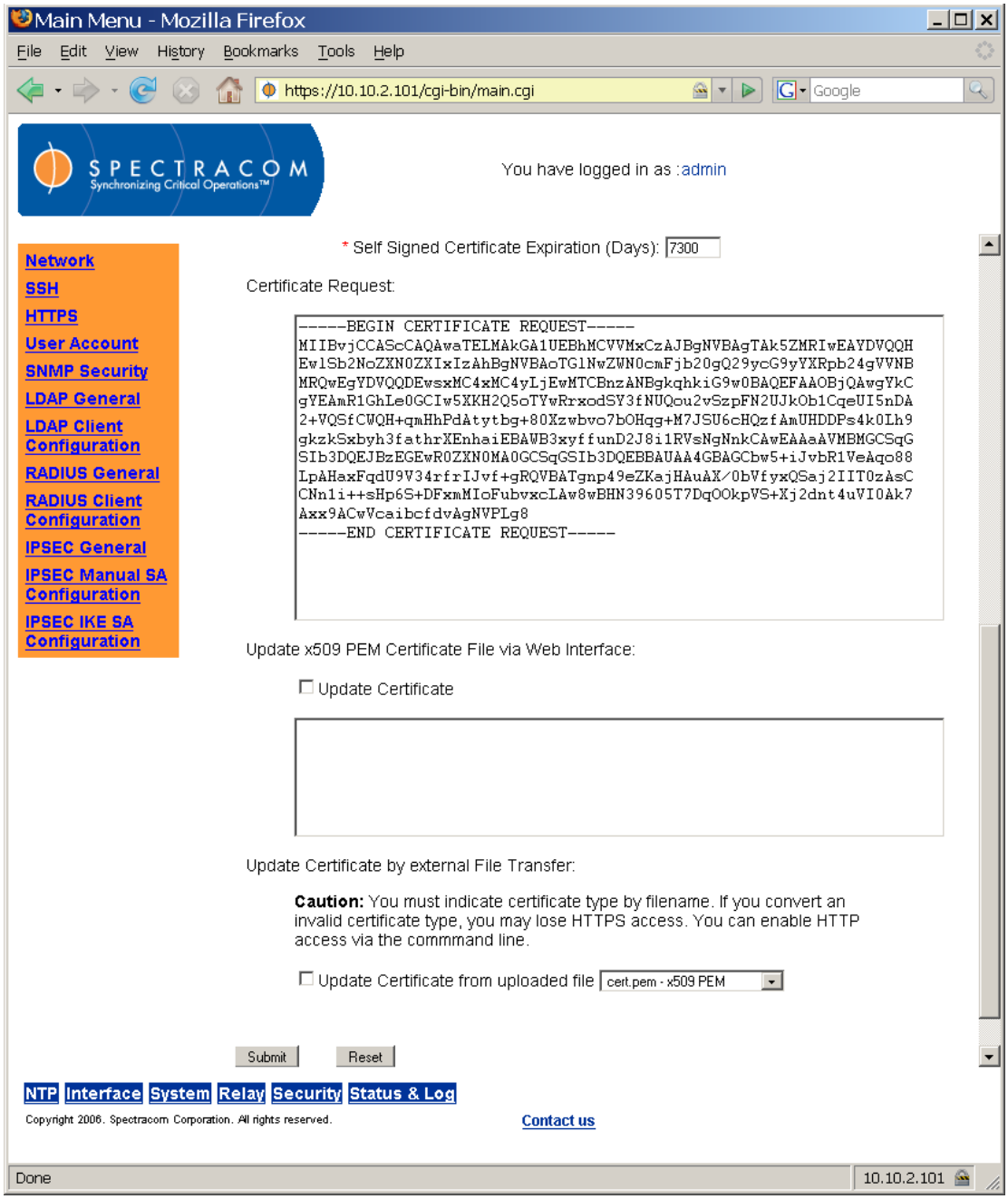


Figure 3-76: Security HTTPS Screen (2 of 2)

NOTE: When generating a certificate, select **Apache** when prompted for information on the Web server's software. This should result in the preferred x509 PEM certificate format.

The Common Name field is the name of the host being authenticated. The Common Name field in the x509 certificate must match the hostname, IP address, or URL used to reach the host via HTTPS. This field should be filled with the hostname or IP address of the NetClock. Spectracom recommends using a static IP address, because DHCP-generated IP addresses can change. If the hostname or IP address changes, the x509 certificate must be regenerated. If using only self-signed certificates, the user should choose the fields based on the company's security policy.

Many certificate authorities simply provide you with a certificate in the form of a plain text file. If your certificate is provided in this manner, and the certificate is provided in the x509 PEM format, you may simply copy and paste the text into the web UI. Paste the text into the "Update Certificate" box, make sure that the Update Certificate checkbox is selected, and submit your changes.

NOTE: Only x509 PEM certificates can be loaded into the Web UI.

3.4.17.5.2 Updating x509 PEM Certificate Files Through External File Transfer

If you are provided with a certificate file and the certificate is **not** in the X509 PEM format, you may use an alternative method to update the certificate. Name the file using the following scheme:

File Type	File Name
x509 PEM	cert.pem
x509 DER	cert.der
pkcs7 PEM	certpem.p7c
pks7c DER	certder.p7c

Next, use an FTP, SCP, or SFTP program to connect to the NetClock. Copy your certificate to the default FTP starting directory. Then select the "Update Certificate from uploaded file" checkbox, select the appropriate file name in the associated drop-down box, and click the "Submit" button.

Be aware that it may take several minutes for the certificate request, the private key, and self-signed certificate are created. The larger the key, the longer amount of time is required. It is recommended that a key bit length be a power of 2 or multiple of 2. The key bit length chosen is typically 1024, but can range from 512 to 4096. Long key bit lengths of up to 4096 are not recommended because they can take hours to generate. The most common key bit length is the value 1024.

The user is provided with several signature algorithm choices. The signature algorithm or message digest is most commonly MD5. Other secure options include SHA1 and RMD160.

Consult your Web Browser documentation and Certificate Authority for key bit lengths and signature algorithms supported.

If a system is rebooted during this time, the certificate will not be created. When the operation is completed, the user will see a certificate request in the certificate request text box. A digital file copy of the certificate request can be found in the root directory with the file name cert.csr. This file can be retrieved using FTP, SCP or SFTP. The certificate request can also be cut and paste from the certificate request text box on the web browser user interface.

3.4.18 If You Cannot Access a Secure NetClock

Spectracom assumes that the customer is responsible for the physical security of the product. Spectracom secure products are required to be locked in a secure enclosure, cabinet or room. Unauthorized persons are not to be given access to the product nor should a serial cable and terminal program be attached unless the system administrator is configuring or performing maintenance.

If your company disables HTTPS, loses the system passwords, allows the certificate to expire, deletes the certificate the certificate and private keys and deletes the Host Keys or forgets the Passphrase access to the secure Spectracom product can become denied.

To restore access to your system you must utilize the setup port to restore the admin accounts default password. The admin account can then be used to enable HTTP using the “net HTTP” command. Contact Spectracom Technical Support for details on how to do this.

3.4.19 Configuring User Accounts

Figure 3-77: Security User Account Screen

From the Security User Account screen (Figure 3-77), the user may create and assign privileges to up to 16 local users. Click “Create/New” and “Submit” to create and assign privileges to users (Figure 3-78).

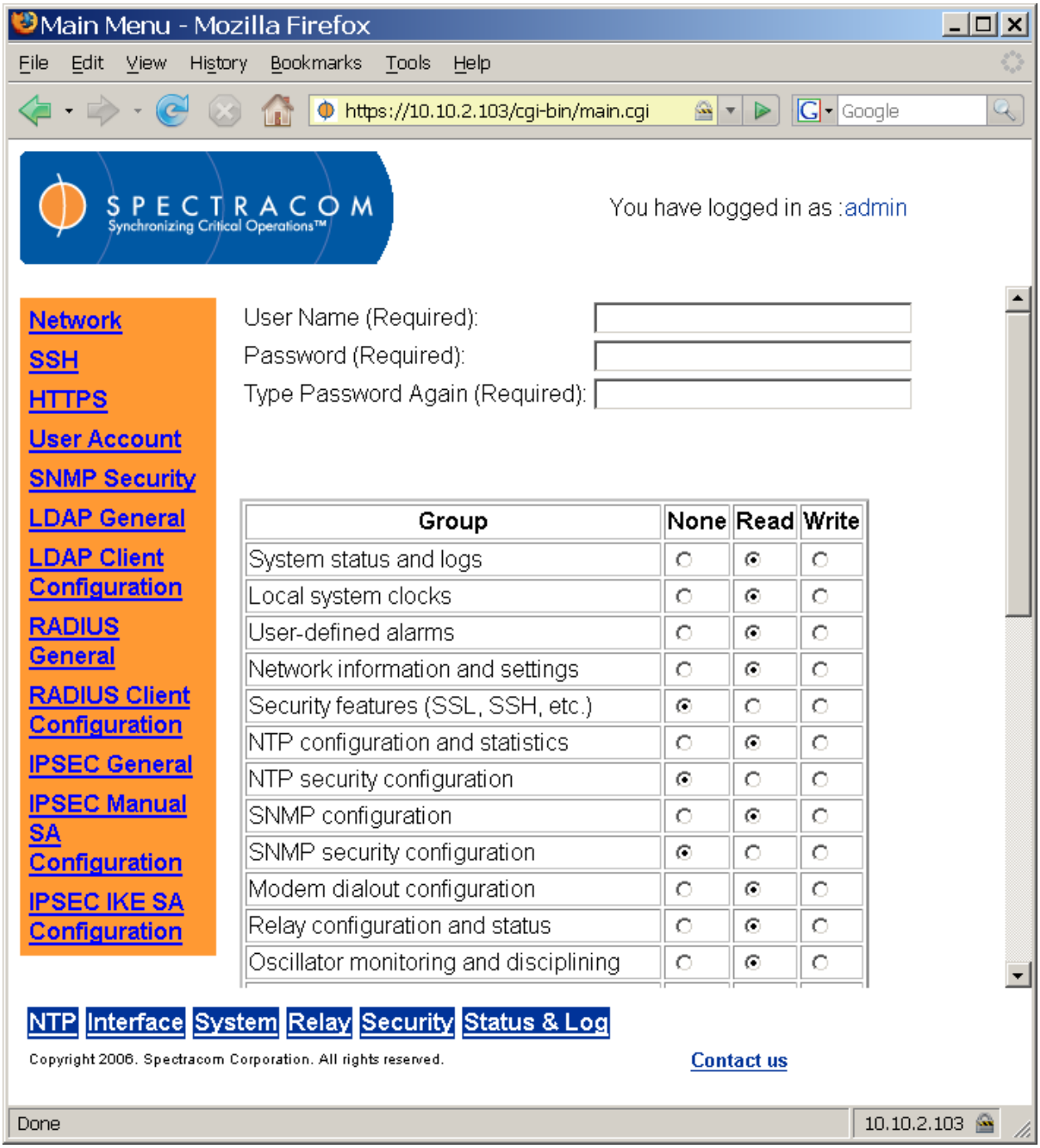


Figure 3-78: Security User Account Screen (Assigning Privileges)

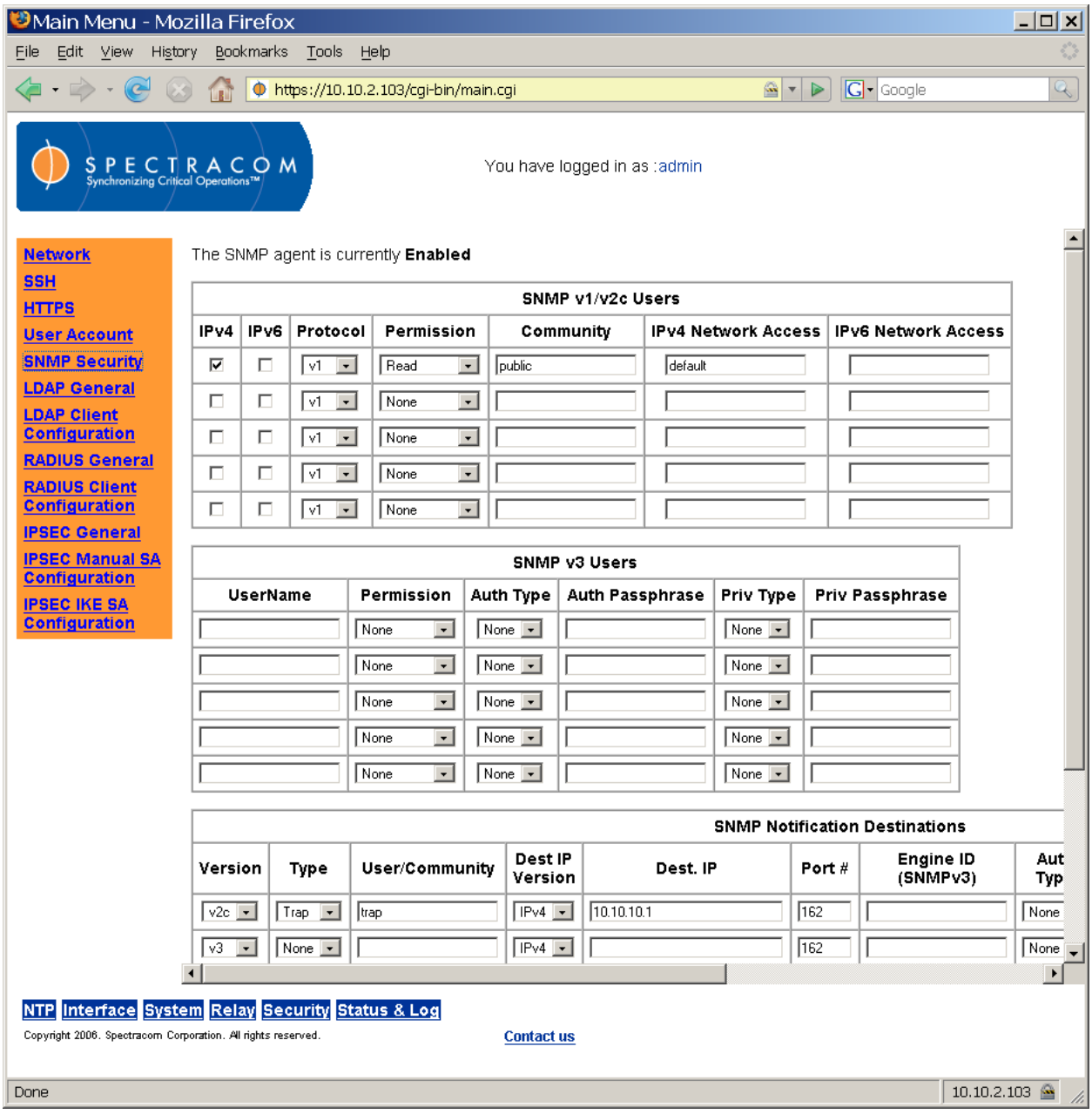

Main Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.10.2.103/cgi-bin/main.cgi
Google
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Network
SSH
HTTPS
User Account
SNMP Security
LDAP General
LDAP Client Configuration
RADIUS General
RADIUS Client Configuration
IPSEC General
IPSEC Manual SA Configuration
IPSEC IKE SA Configuration
The SNMP agent is currently Enabled
SNMP v1/v2c Users
IPv4 IPv6 Protocol Permission Community IPv4 Network Access IPv6 Network Access
public default
SNMP v3 Users
UserName Permission Auth Type Auth Passphrase Priv Type Priv Passphrase
SNMP Notification Destinations
Version Type User/Community Dest IP Version Dest. IP Port # Engine ID (SNMPv3) Aut Typ
v2c Trap trap IPv4 10.10.10.1 162 None
v3 None IPv4 162 None
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Done
10.10.2.103

Figure 3-79: SNMP Security Screen (1 of 3)

3.4.20 Configuring SNMP v1, v2, and v3

From the SNMP Security screen (Figure 3-79), the user can define the network locations, hostnames, and protocols used in communicating with SNMP v1, v2, and v3 users. (SNMP v3 is secure SNMP.)

NOTE: Usernames are arbitrary. The username must be the same on the unit and on the management station.

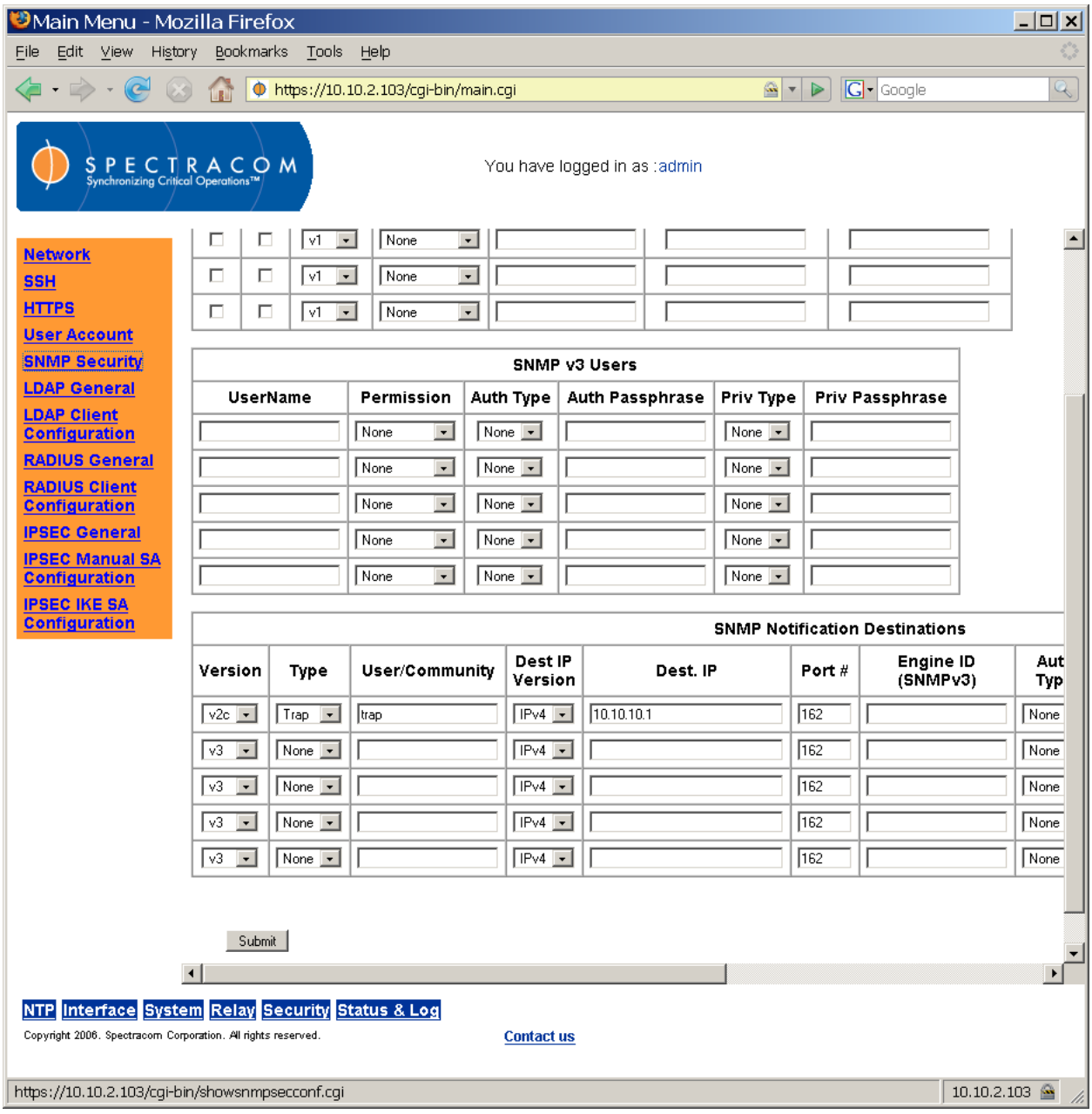


Figure 3-80: SNMP Security Screen (2 of 3)

NOTE: When selecting an engine ID for SNMPv3, pick an arbitrary hexadecimal number (such as 0x1234).

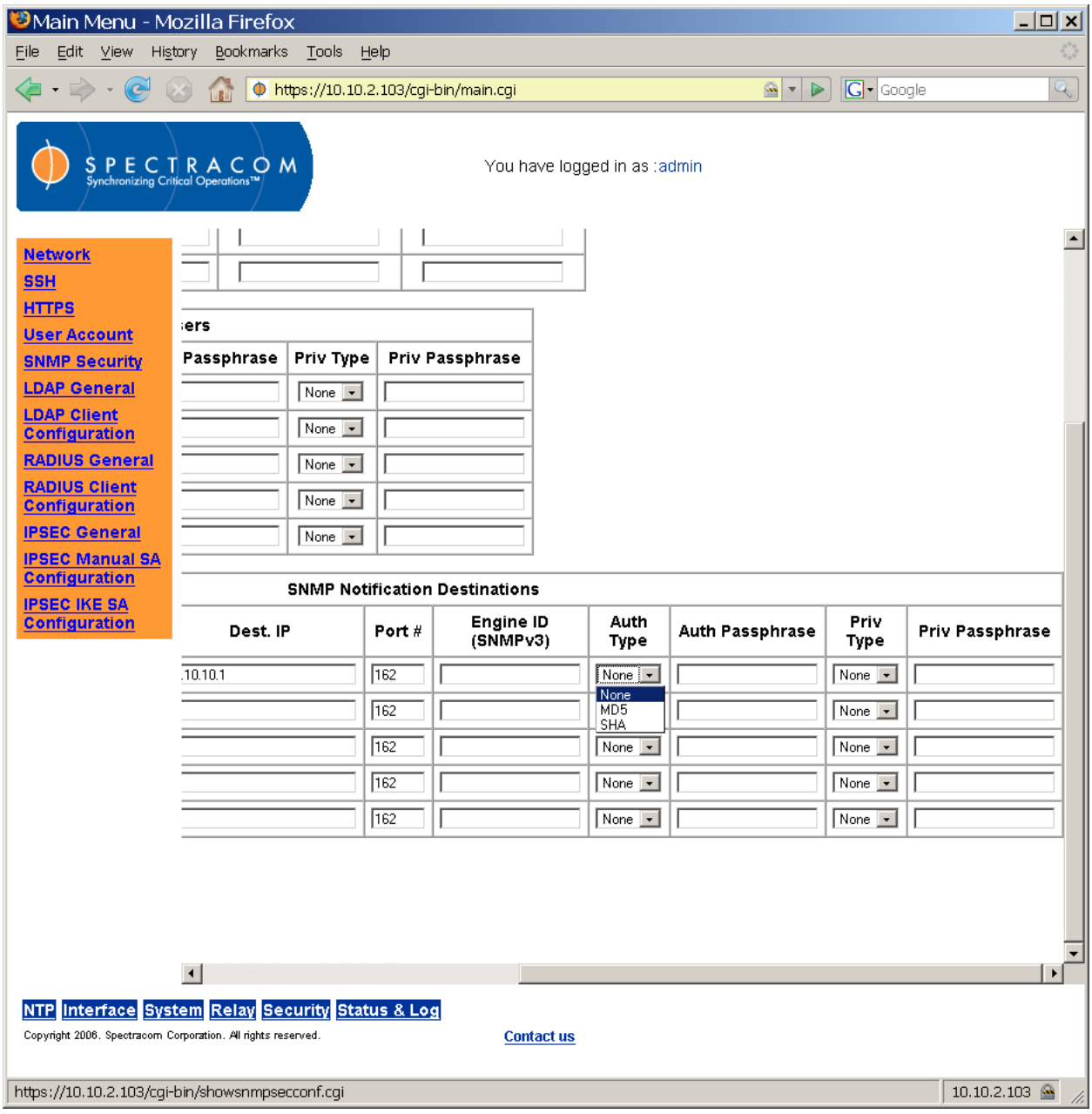


Figure 3-81: SNMP Security Screen (3 of 3)

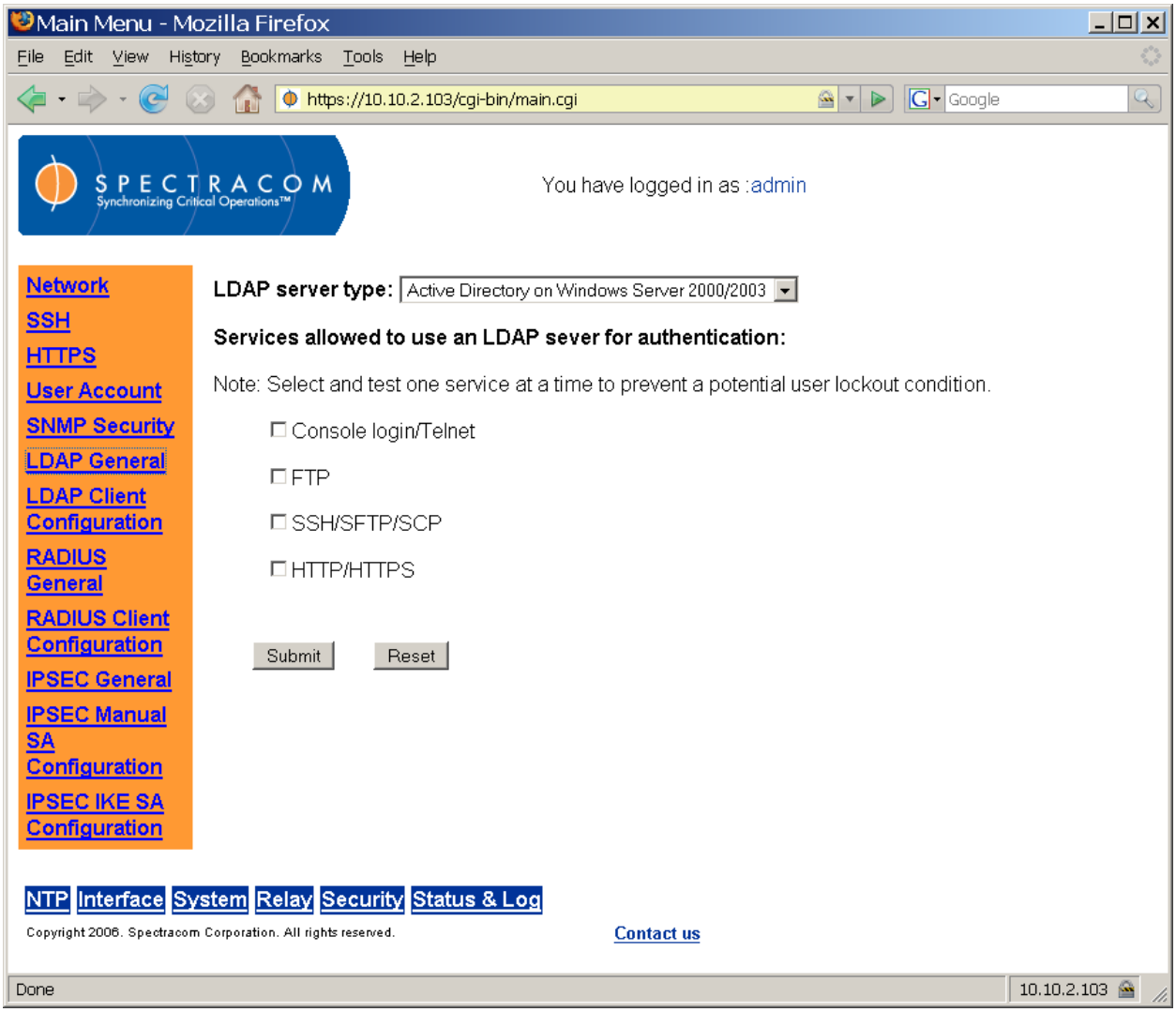


Figure 3-82: Security LDAP General Screen

3.4.21 Configuring LDAP and RADIUS

From the Security LDAP General screen (Figure 3-82), the user chooses the LDAP server type (it must be the correct one – check with your LDAP server administrator if you are not sure) and choose the types of services allowed to request authentication from the LDAP server.

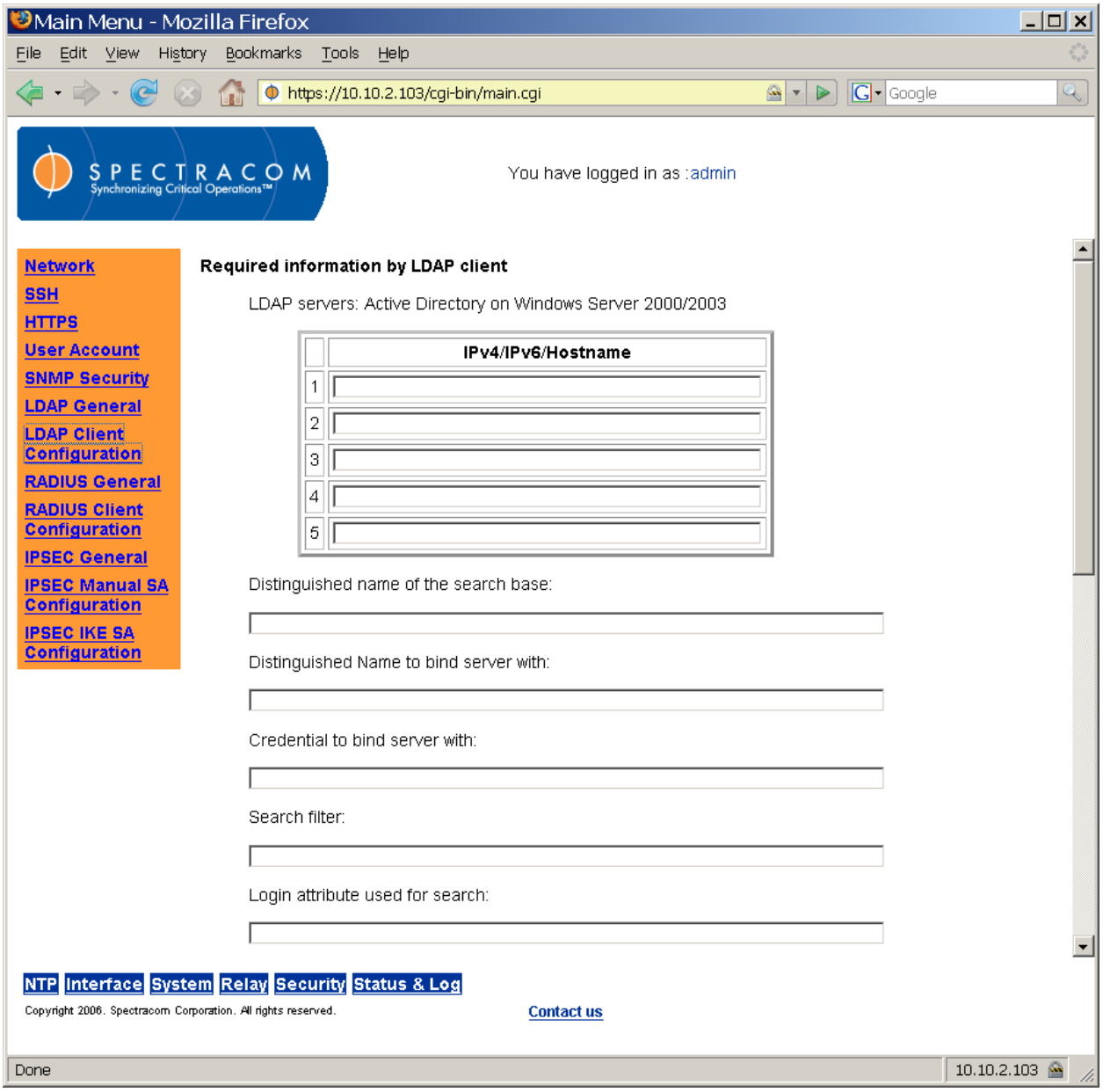


Figure 3-83: Security LDAP Client Configuration Screen (1 of 2)

From the LDAP Client Configuration screen, the user specifies the addresses or hostnames of the LDAP server(s) and inputs other fields that must be provided by the LDAP server administrator. One of the servers (and one only) must be defined as the main LDAP server. The other servers are replicas.

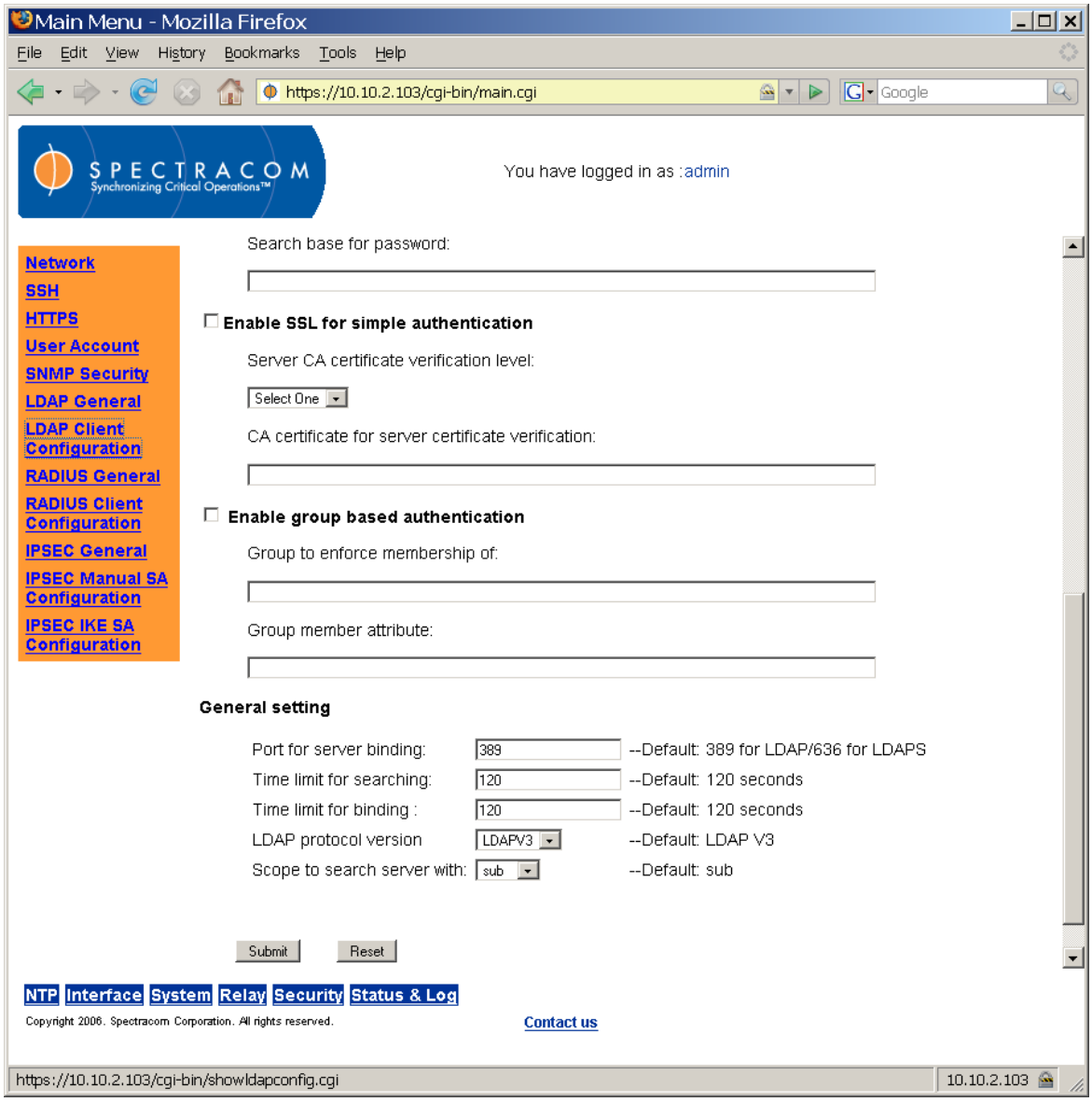


Figure 3-84: Security LDAP Client Configuration Screen (2 of 2)

If “Enable SSL for simple authentication” is not clicked, clear text is sent to the LDAP server. If SSL is checked, text sent to the LDAP server is encrypted.

A sample configuration for an OpenLDAP server would be as follows:

DN for search base	dc=spectracomcorp,dc=com
Bind DN	cn=manager,dc=spectracomcorp,dc=com
Bind password	test
Search filter	objectclass=posixaccount
Login attribute	uid
DN for password	ou=people,dc=spectracomcorp,dc=com?one
Group DN	cn=engineer,ou=group,dc=spectracomcorp,dc=com
Group member attribute	member

A sample configuration for Active Directory would be as follows:

DN for search base	dc=test,dc=spectracomcorp,dc=com
Bind DN	cn=administrator,cn=users,dc=test,dc=spectracomcorp,dc=com
Bind password	test
Search filter	objectclass=User
Login attribute	sAMAccountName
DN for password	ou=users,dc=test,dc=spectracomcorp,dc=com?one
Group DN	cn=engineer,cn=users,dc=test,dc=spectracomcorp,dc=com
Group member attribute	member

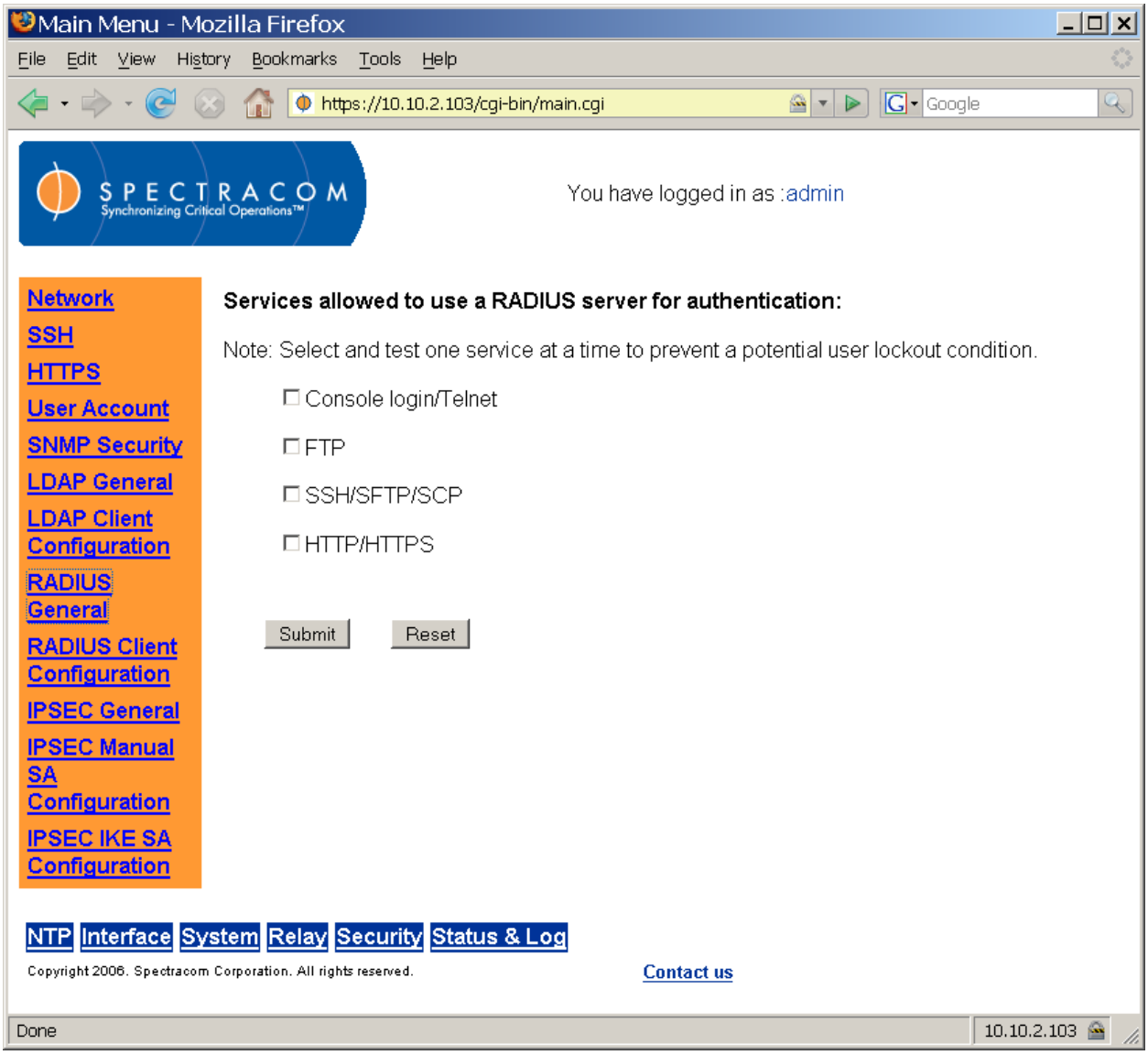


Figure 3-85: Security RADIUS General Screen

From the Security RADIUS General screen (Figure 3-85), the user selects the services that may use RADIUS for authentication.

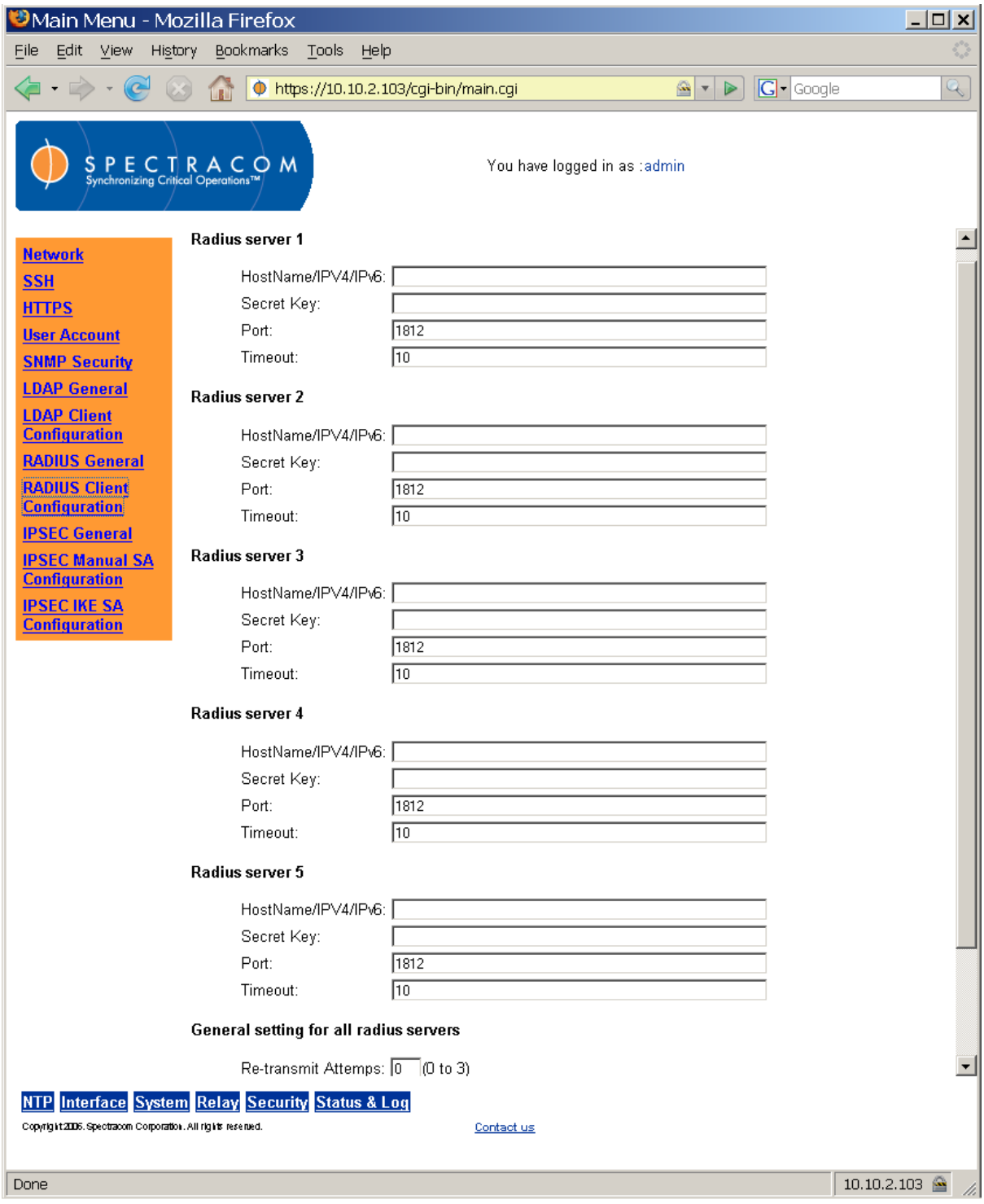


Figure 3-86: Security RADIUS Client Configuration Screen

From the Security RADIUS Client Configuration screen (Figure 3-86), the user identifies the addresses of the network's RADIUS servers. From this screen, the user also specifies the number of re-transmit attempts (0 to 3) that will be made in communicating with the RADIUS server.

3.4.22 Configuring IPSec

Internet Protocol Security (IPSec) is a suite of IP protocols that authenticates and encrypts network communications. IPSec supports IPv6 and IPv4 as of this writing.

IPSec defines a Security Association (SA), consisting of secured communications between two network devices. Configuring IPSec requires us to define SA Policy (SAP) and SA Descriptors (SAD). SAP determines what network traffic can or must be secured through IPSec. SAD describes actively secured conversations. All network traffic for an SA contains an identical Security Parameter Index (SPI).

3.4.22.1 AH vs. ESP

An Authentication Header (AH) and an Encapsulating Security Payload (ESP) are the primary protocols used by IPSec. They authenticate (AH) or authenticate and encrypt (ESP) the data across that connection. Typically, they are used independently, but it is possible to use them together. The NetClock supports both protocols.

3.4.22.2 Transport Mode vs. Tunnel Mode

Transport mode provides a secure connection between two endpoints by encapsulating the IP payload. Tunnel mode encapsulates the entire IP packet/

NOTE: Tunnel mode is used to form a traditional Virtual Private Network (VPN), in which the tunnel creates a secure path across a distrusted Internet connection. The NetClock supports *Transport mode ONLY.*

3.4.22.3 MD5 vs. SHA-1 vs. DES vs. 3DES vs. AES

An IPSec connection can use two or three encryption choices from among those available. Authentication calculates an Integrity Check Value (ICV) over the data packet's contents. It is usually built on a hash algorithm (for example, MD5 or SHA-1). It uses a secure key known to both endpoints, allowing the recipient to compute the ICV as the sender has computed it. If the recipient gets the same value, the sender has effectively authenticated itself.

3.4.22.4 IKE vs. Manual Keys

To communicate, the devices at both endpoints must possess the same secure keys. Keys can be entered manually. They may also be generated dynamically between two hosts through Internet Key Exchange (IKE). The NetClock supports both IKE and manual keys.

3.4.22.5 Main Mode vs. Aggressive Mode

The initial IKE exchange may be efficient or it may be secure. This tradeoff is governed by the exchange mode, Main or Aggressive. Main mode is completely secure and requires six packets to be sent between the two devices. Aggressive mode requires only three packets be sent between the two devices, but it is less secure.

NOTE: The NetClock supports both Main and Aggressive modes. Aggressive mode is NOT recommended because of the security risks involved.

3.4.22.6 Configuring IPSec (IKE SA)

To establish an IPSec connection between the Spectracom NetClock and an IPv4 addressed host (“A”) using IKE SA configuration, we must first configure the IPSec IKE to communicate with host A. To do this, navigate to the IPSEC IKE SA Configuration screen (Figure 3-87).

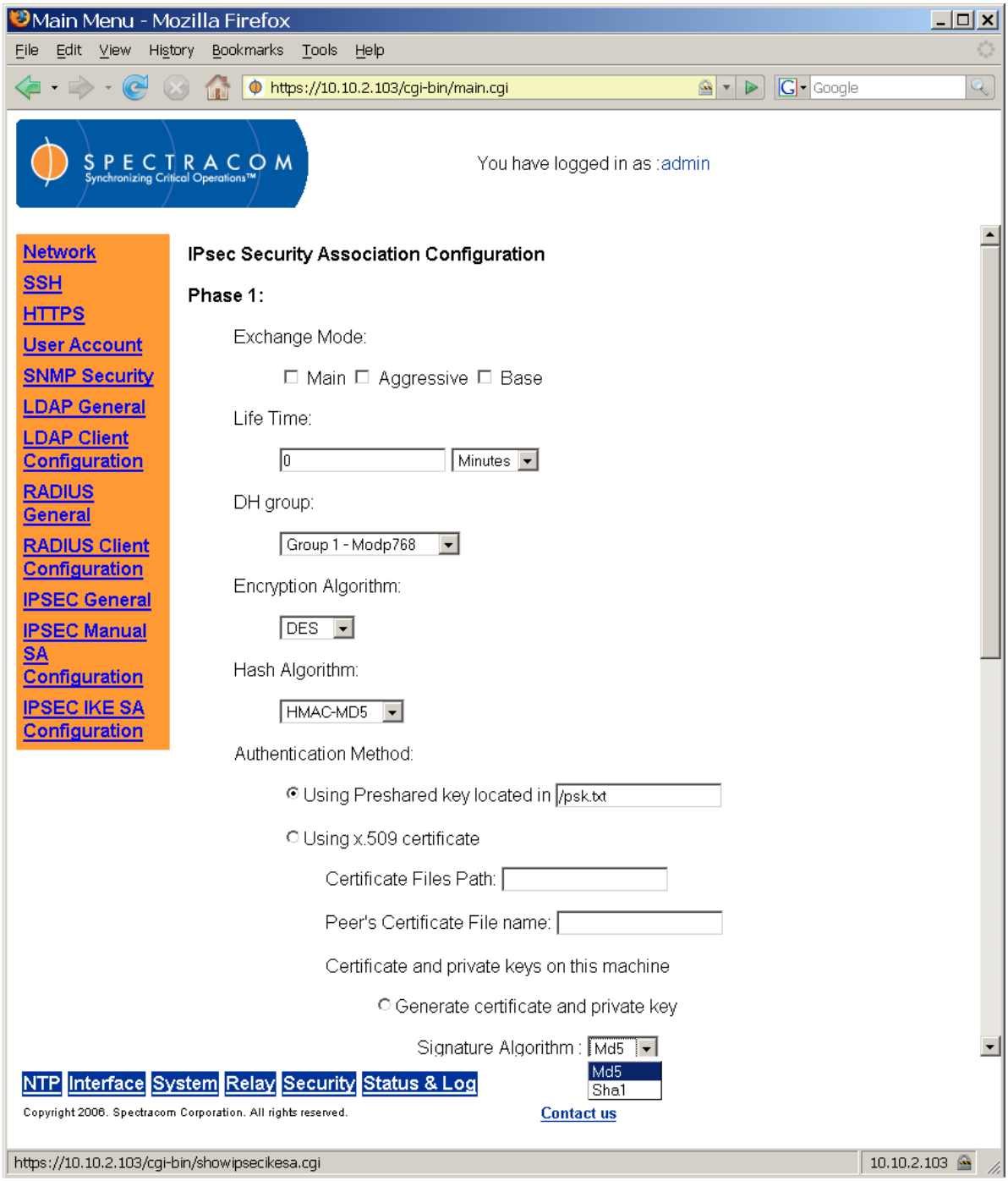


Figure 3-87: IPSEC IKE SA Configuration Screen (1 of 2)

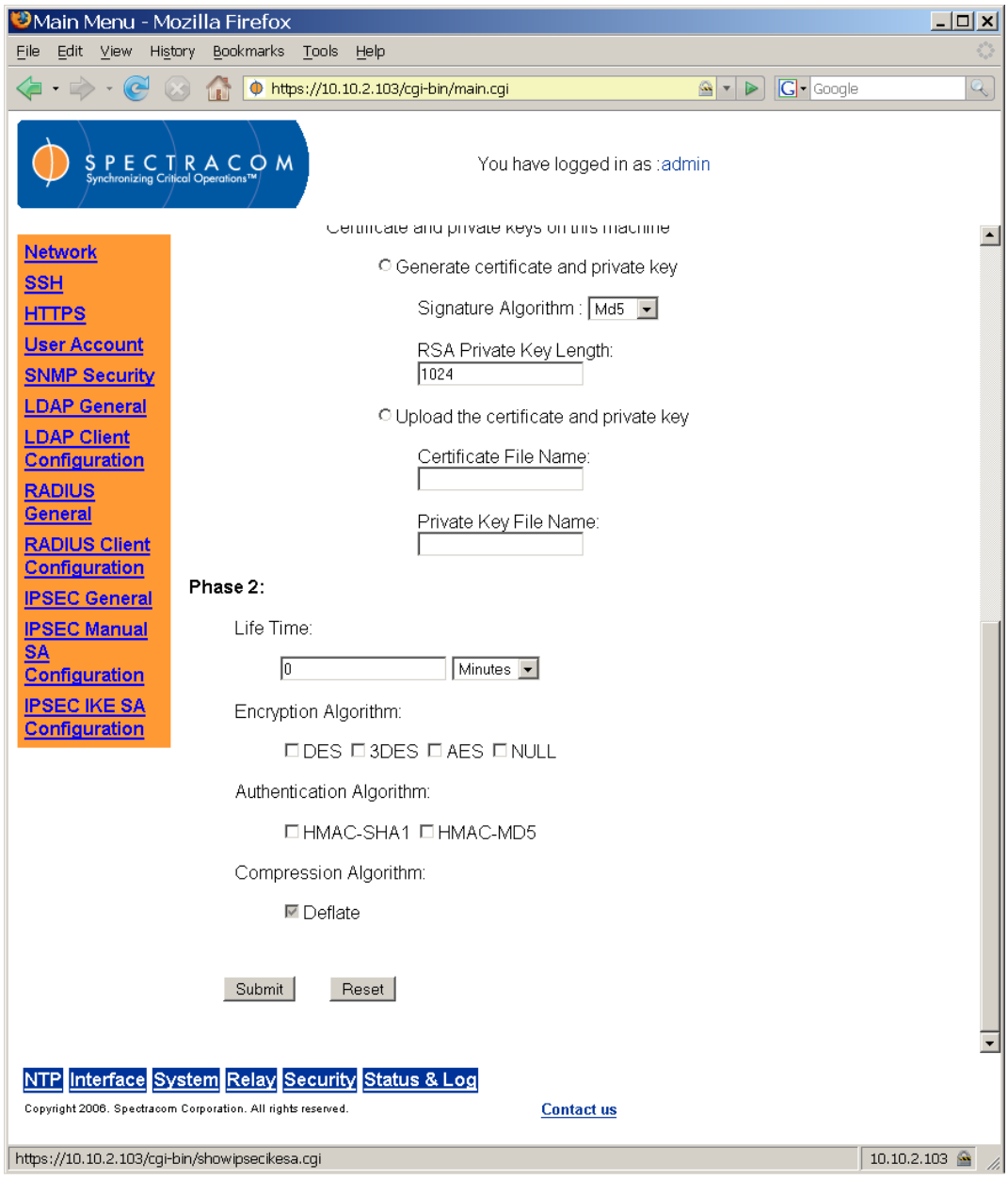


Figure 3-88: IPSEC IKE SA Configuration Screen (2 of 2)

3.4.22.6.1 IKE Phase 1 Configuration

Exchange Mode defines the mode for Phase 1 (when the IKE daemon is the initiator). You may select all three options (meaning the NetClock supports Main, Aggressive, and Base exchange modes) or you may select one or two modes to support. The IKE daemon uses the Main exchange mode when it is the initiator.

Life Time defines the lifetime of the Phase 1 SA proposal.

DH group defines the group used for Diffie-Hellman exponentiations. This directive must be defined using one of the following:

Group 1 - Modp768
Group 2 - Modp1024
Group 5 - Modp1536
Grouip 14 - Modp2048

NOTE: When using Aggressive mode, the DH group defined for each proposal must be the same.

Encryption Algorithm specifies the algorithm used for Phase 1 negotiation. Choose DES, 3DES, or AES as desired (or as specified by your network administrator).

Hash Algorithm defines another algorithm used for Phase 1 negotiation. Select HMAC-MD5 or HMAC-SHA1 as desired or required.

Authentication Method defines the means of Phase 1 authentication used (preshared keys or X.509 certificates).

Preshared Keys

The easiest way to authenticate using the IKE daemon is through preshared keys. These keys must be defined in a file uploaded to the location specified in the *Using Preshared key located in* field.

NOTE: After the file is uploaded, its file privileges will be changed automatically to deny unauthorized users access to the preshared keys. This means you will not be able to access the file after uploading it. Always keep an extra copy of the file on hand in another location.

The preshared key file should have the following syntax:

```
192.168.2.100          password1
5.0.0.1                password2
3ffe:501:ffff::3       password3
```

This file is organized in columns. The first column holds the identity of the peer authenticated by the preshared key. The second column contains the keys.

X.509 Certificates

The IKE daemon supports the use of X.509 certificates for authentication. Spectram supplies two means of providing the public/private key pair to the NetClock.

The first approach is through the user interface on the IPSec IKE SA Configuration screen. Specify the Certificate Files Path and Peer's Certificate File name, then select Md5 or Sha1 to specify the Signature Algorithm. You must also specify the RSA Private Key Length to use when generating the key pair.

Alternatively, you may generate elsewhere and upload to the NetClock your key pair(s). Specify the directory and the name of the key pairs uploaded to it. Regardless of the method used, however, you must upload the peer's public key to the NetClock and provide the directory and file name to the NetClock in the IPSec IKE SA Configuration screen.

3.4.22.6.2 IKE Phase 2 Configuration

Life Time defines how long an IPSec SA will be used.

Encryption Algorithm defines the group used for Diffie-Hellman exponentiations. This directive must be defined using one of the following:

Group 1 - Modp768
Group 2 - Modp1024
Group 5 - Modp1536
Grouip 14 - Modp2048

NOTE: When using Aggressive mode, the DH group defined for each proposal must be the same.

Encryption Algorithm specifies the algorithm used for Phase 2. Select DES, 3DES, AES (used with ESP) or NULL as desired (or as required by your network administrator).

Authentication Algorithm defines another algorithm used for Phase 2. Select HMAC-SHA1 or HMAC-MD5 as desired or required.

Compression Algorithm defaults to "deflate." It is not configurable at this time.

NOTE: After completing and submitting changes in the IPSec IKE SA Configuration screen, check to make sure IPSec is enabled and IKE is selected for use with IPSec. The IKE Log (refer to *Logs and Status Reporting*) is helpful in troubleshooting this condition.

3.4.22.6.3 Configure IPSec Security Policy

Configure the IPSec security policy from the IPSec General screen (Figure 3-89).

NOTE: Always configure IKE BEFORE enabling the IKE option from the IPSec General screen. If IKE is not configured, the IKE daemon won't start correctly when the Security Association is enabled.

From the IPSec General screen (Figure 3-89), enable (or disable) the IPSec service and specify the Security Association (IKE if already configured, or Manually Configure). In the Security Policy table, input the NetClock's IP address as the Source IP and host A's address as the Destination IP.

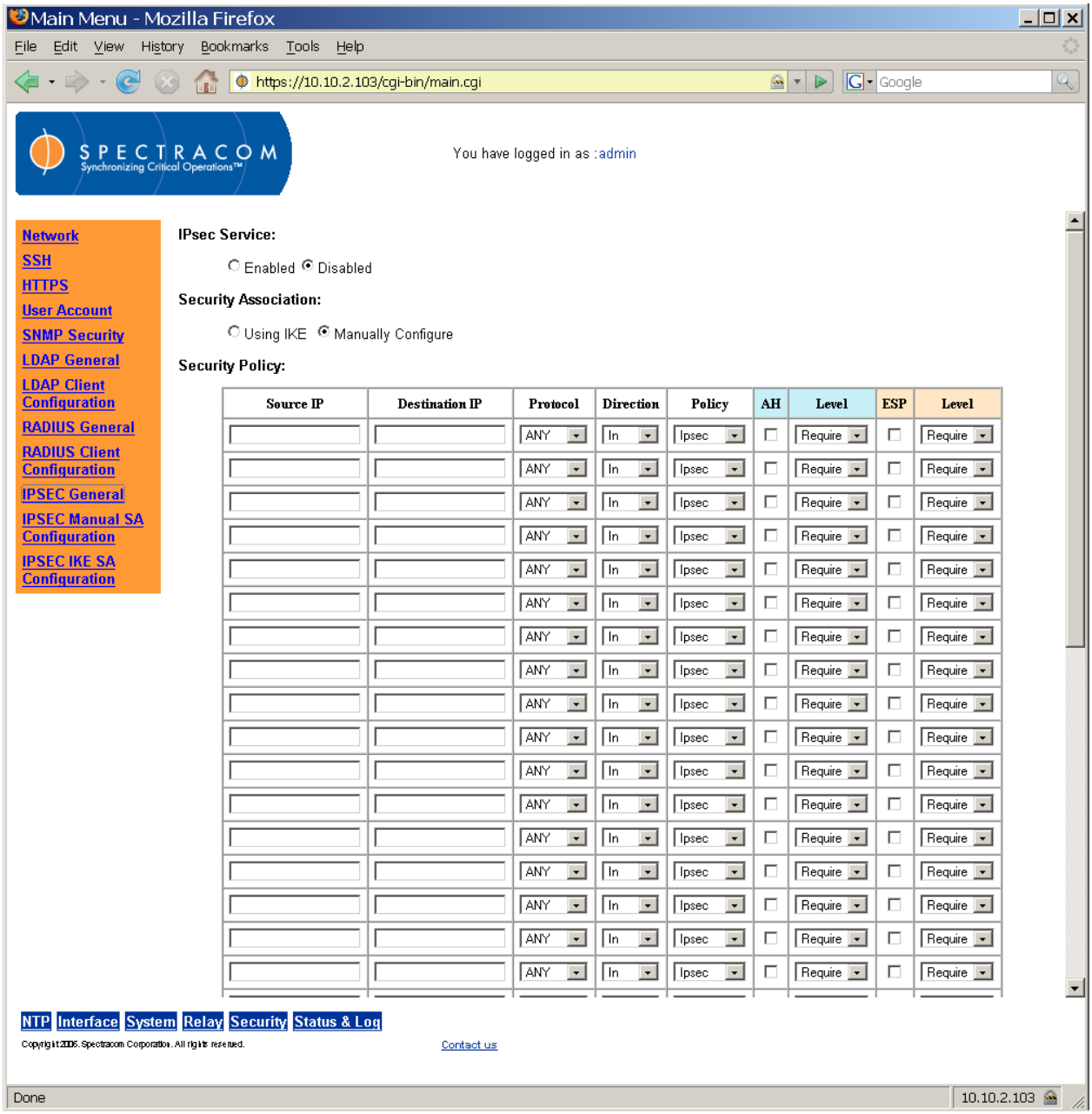


Figure 3-89: IPSec General Screen

Select *ANY* as the desired protocol to apply for IPSec security protection (unless a specific protocol is desired; these can be selected from the drop-down list).

Select *Both* for the Direction, which means IPSec security protection is required for both incoming and outgoing packets. Security protection may also be applied to incoming packets only, or to outgoing packets only (from the drop-down list).

Select *Ipsec* to use IPSec as the security policy. (You may also select *None* or *Discard*. Selecting *None* means that IPSec operation will not take place on the packet, while selecting *Discard* means the packet matching indexes will be discarded.

You may choose to check either or both AH and ESP to set them as *Require*, *Use*, *Default*, or *Unique*.

- *Default* means the kernel consults the system-wide default for the protocol specified.
- *Use* means the kernel uses an SA if it is available, while the kernel keeps normal operation otherwise.
- *Require* means an SA is required whenever the kernel sends a packet matched with the policy.
- *Unique* is the same as Require, but allows the policy to match the unique outbound SA.

3.4.22.7 Configuring IPSec (Manual SA)

To establish an IPSec connection between the NetClcok and an IPv6 addressed host (“B”) using manual SA configuration, refer to the IPSec Manual SA Configuration screen (Figure 3-90).

3.4.22.7.1 Manual Security Associations

Input the NetClock IP address as the Source IP and host B’s IP address as the Destination IP.

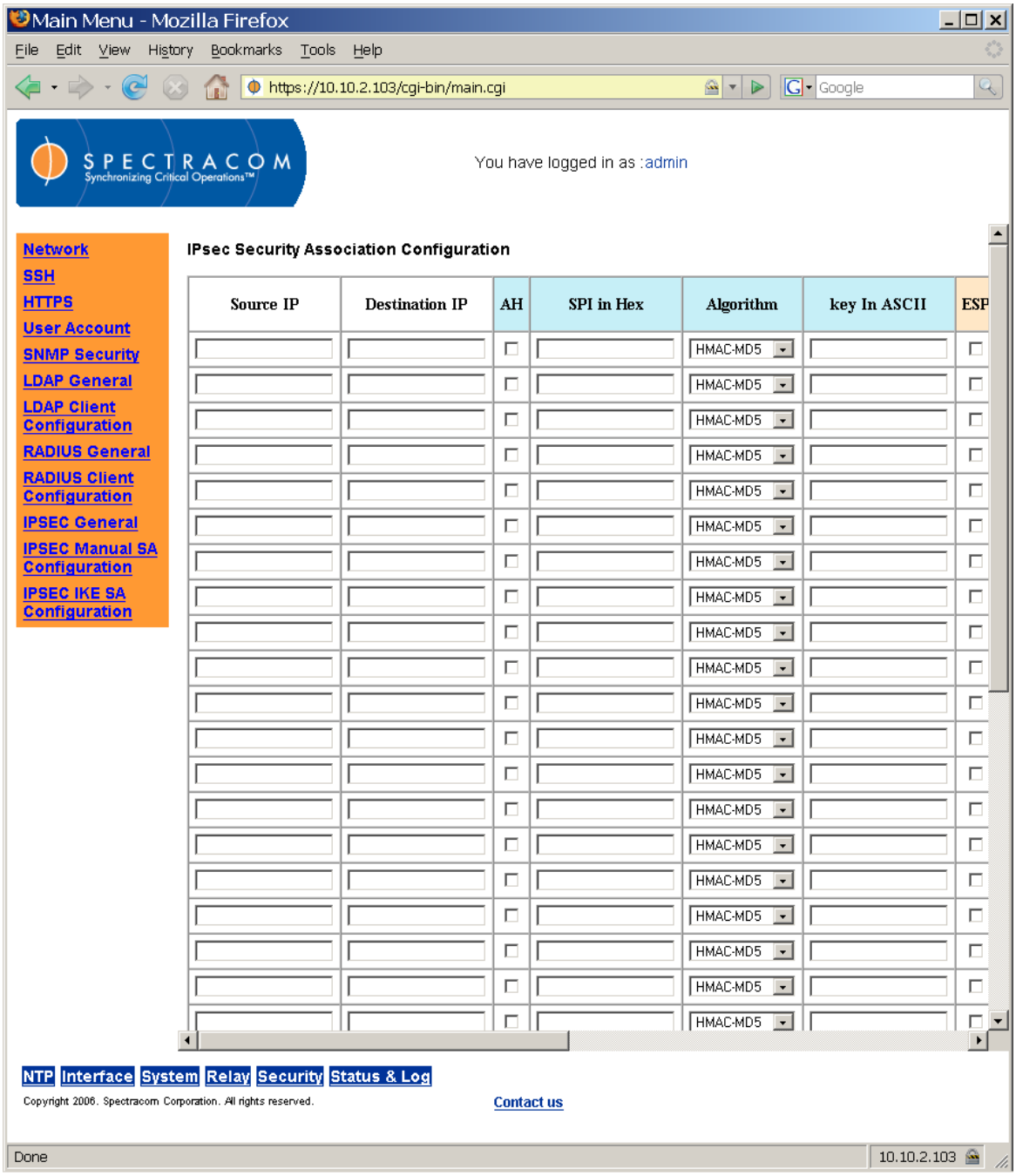


Figure 3-90: IPSec Manual SA Configuration (1 of 2)

The Security Parameter Index (SPI) must be a hexadecimal number without the “0x” prefix. Enter the desired values manually.

NOTE: SPI values between 0 and 255 are reserved and cannot be used at this time.

Make sure to check the AH or ESP boxes for the key configurations used. If the appropriate box is not checked, information following the AH or ESP inputs will be ignored by the update page.

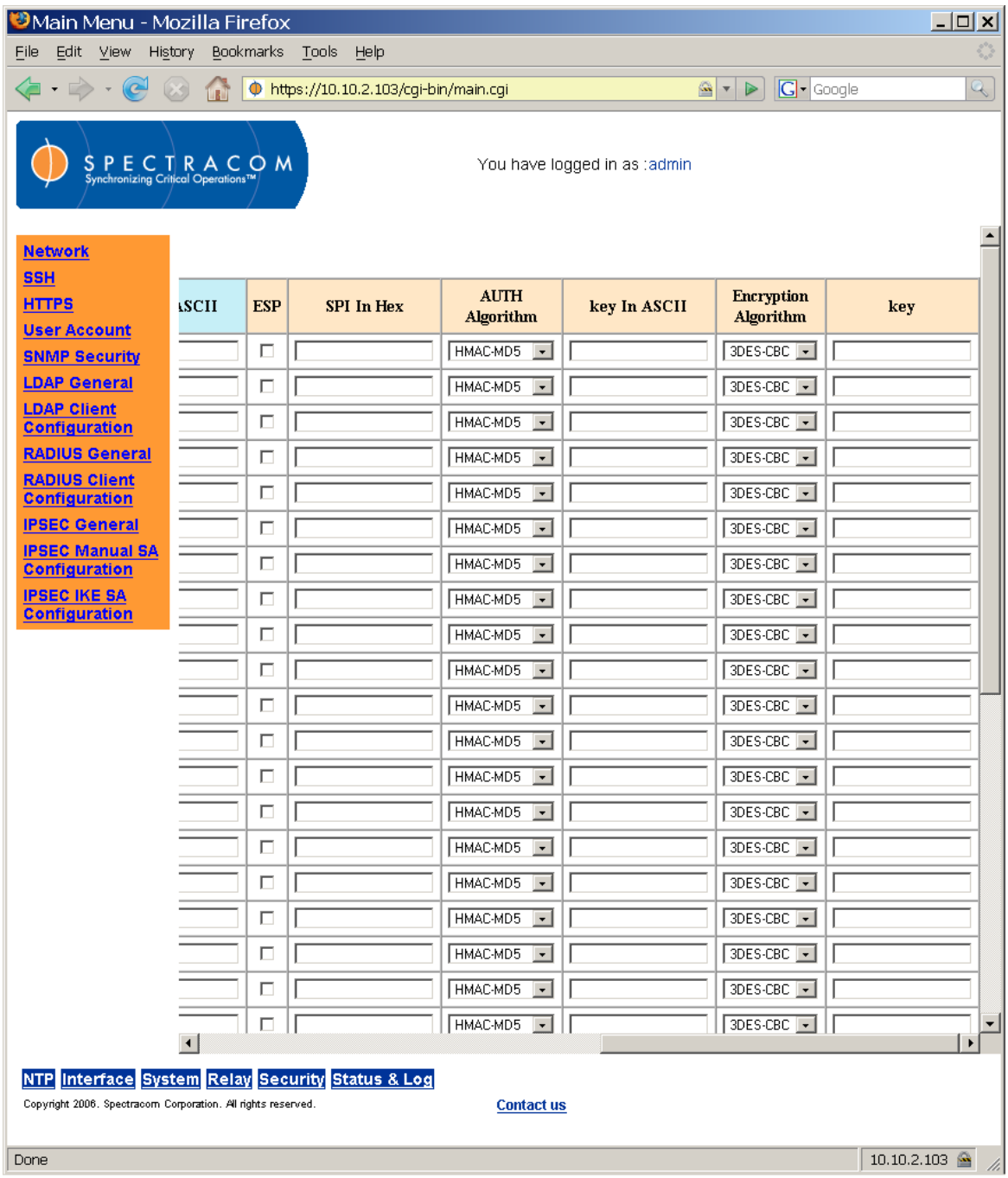


Figure 3-91: IPSec Manual SA Configuration (2 of 2)

3.4.22.7.2 Configure IPSec Security Policy

Configure the IPSec security policy from the IPSec General screen (Figure 3-92).

NOTE: The manual SA values must be configured BEFORE the manual SA option is enabled from the IPSec General screen (Figure 3-92). If the feature is enabled before it is configured from the IPSec Manual SA Configuration screen, the SA and SP tables will not update correctly.

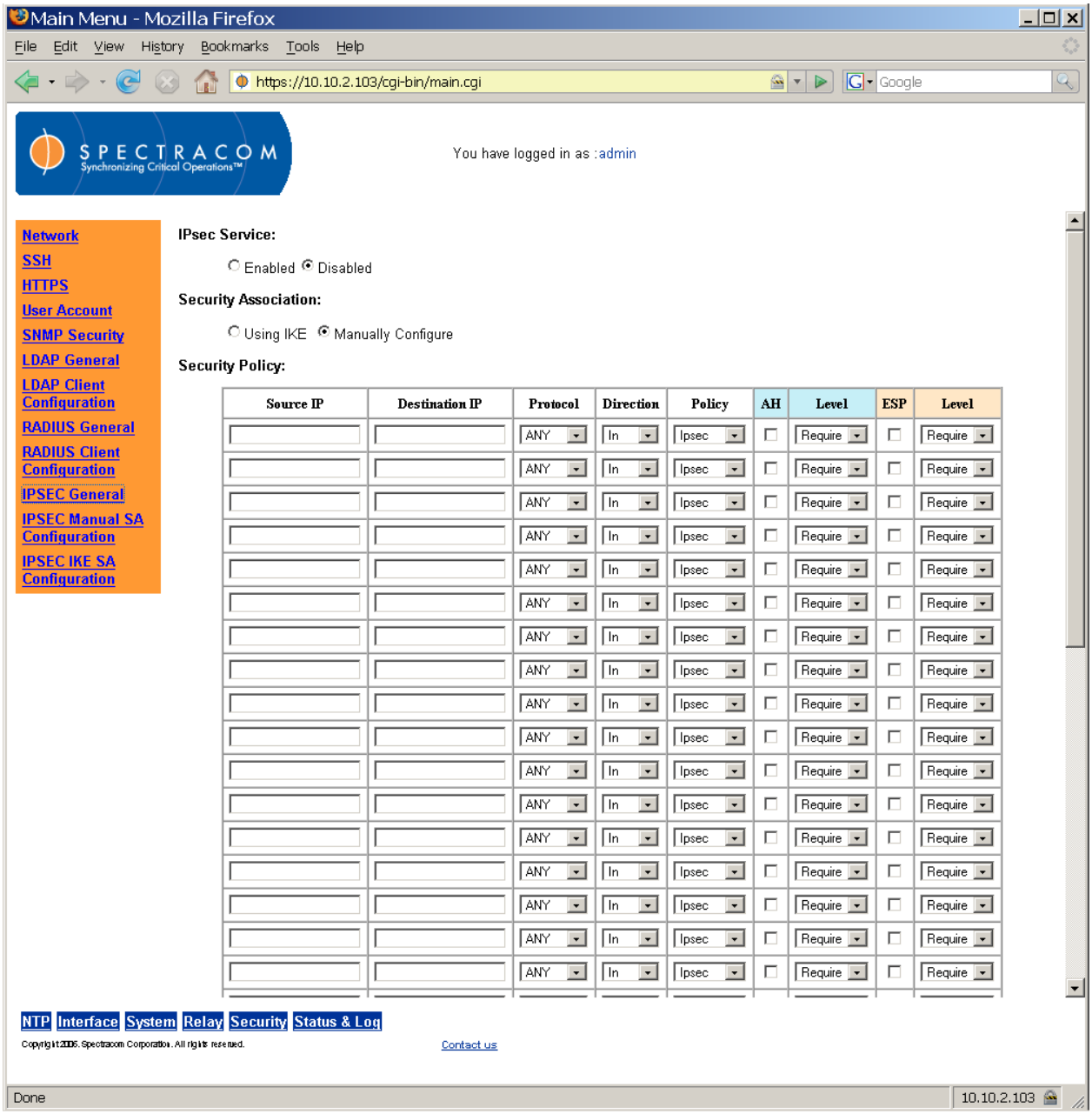


Figure 3-92: IPSec General Screen

Select *ANY* as the desired protocol to apply for IPSec security protection (unless a specific protocol is desired; these can be selected from the drop-down list).

NOTE: When using IKE over IPv6, do NOT select ANY. There are protocols that do not work well with IKE under IPv6 with IKE. Select one of the specific protocols listed in the dropdown menu, as desired or required.

Select *Both* for the Direction, which means IPSec security protection is required for both incoming and outgoing packets. Security protection may also be applied to incoming packets only, or to outgoing packets only (from the drop-down list).

Select *Ipsec* to use IPSec as the security policy. (You may also select *None* or *Discard*. Selecting *None* means that IPSec operation will not take place on the packet, while selecting *Discard* means the packet matching indexes will be discarded.

You may choose to check either or both AH and ESP to set them as *Require*, *Use*, *Default*, or *Unique*.

- *Default* means the kernel consults the system-wide default for the protocol specified.
- *Use* means the kernel uses an SA if it is available, while the kernel keeps normal operation otherwise.
- *Require* means an SA is required whenever the kernel sends a packet matched with the policy.
- *Unique* is the same as Require, but allows the policy to match the unique outbound SA.

3.4.23 Logs and Status Reporting

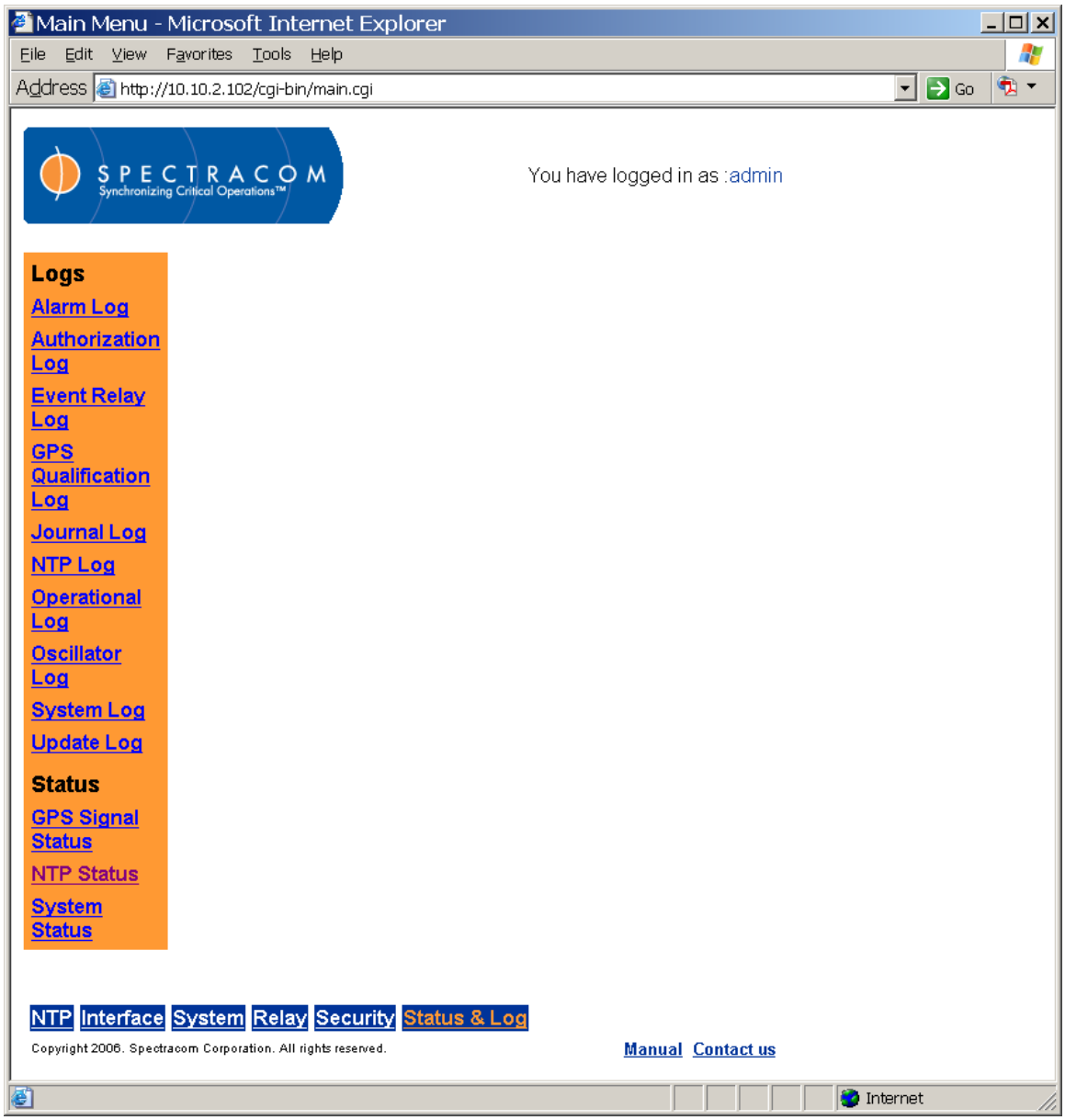


Figure 3-93: Status and Log Menu

The Status and Log menu groups the NetClock's status and log access screens. From this menu the user can view system logs and monitor that status of the NetClock's GPS signal. The user may also view system and NTP statuses from this menu.

NOTE: The times indicated in all log entries are UTC (no correction for local time or Daylight Saving Time). Four iterations of each log are kept locally on the NetClock, with the oldest rotated out (deleted) as a fifth log is generated. Logs can be up to 75K in size individually. This means that 300K of storage is devoted to each log.

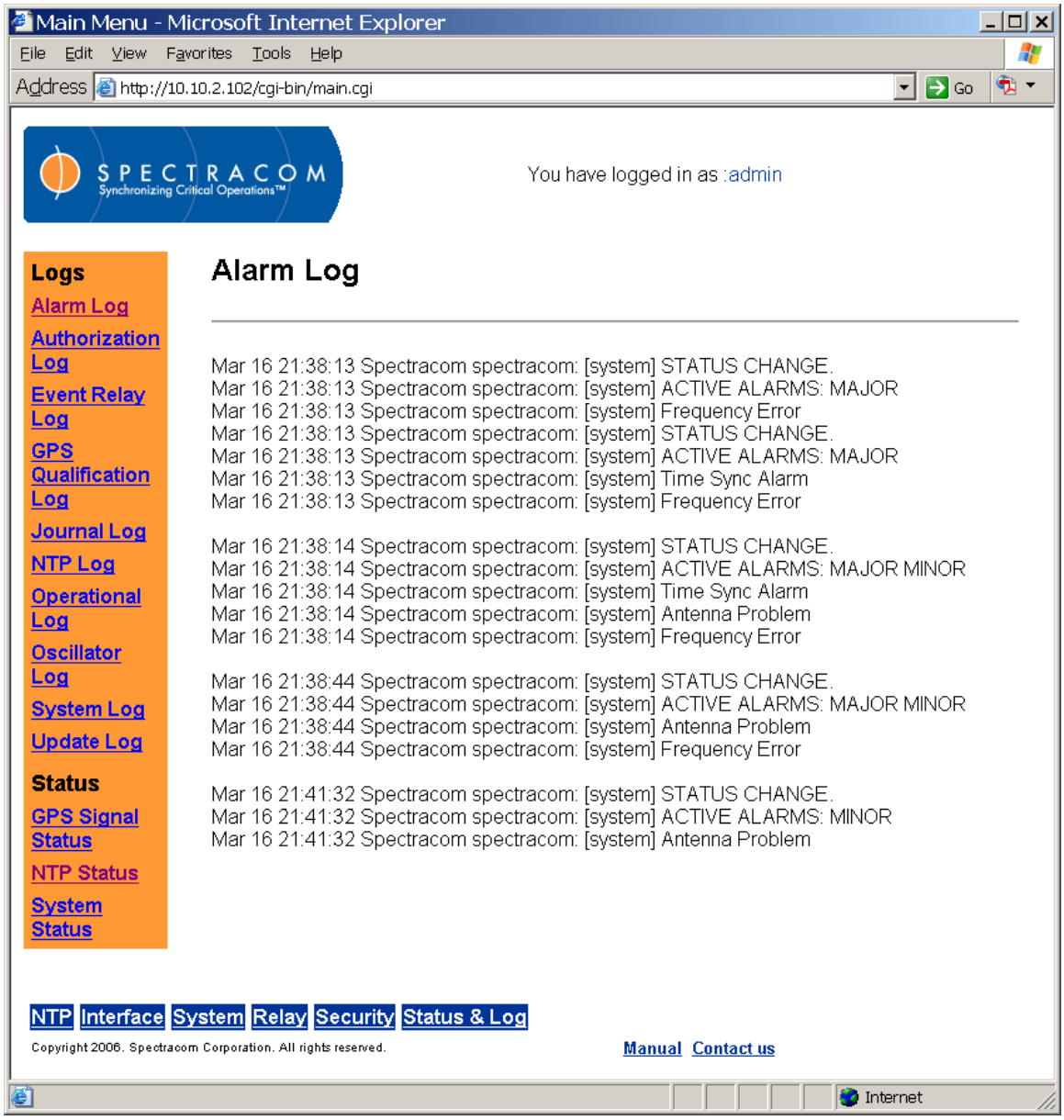

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
Alarm Log
Authorization Log
Event Relay Log
GPS Qualification Log
Journal Log
NTP Log
Operational Log
Oscillator Log
System Log
Update Log
Status
GPS Signal Status
NTP Status
System Status
Alarm Log
Mar 16 21:38:13 Spectracom spectracom: [system] STATUS CHANGE.
Mar 16 21:38:13 Spectracom spectracom: [system] ACTIVE ALARMS: MAJOR
Mar 16 21:38:13 Spectracom spectracom: [system] Frequency Error
Mar 16 21:38:13 Spectracom spectracom: [system] STATUS CHANGE.
Mar 16 21:38:13 Spectracom spectracom: [system] ACTIVE ALARMS: MAJOR
Mar 16 21:38:13 Spectracom spectracom: [system] Time Sync Alarm
Mar 16 21:38:13 Spectracom spectracom: [system] Frequency Error
Mar 16 21:38:14 Spectracom spectracom: [system] STATUS CHANGE.
Mar 16 21:38:14 Spectracom spectracom: [system] ACTIVE ALARMS: MAJOR MINOR
Mar 16 21:38:14 Spectracom spectracom: [system] Time Sync Alarm
Mar 16 21:38:14 Spectracom spectracom: [system] Antenna Problem
Mar 16 21:38:14 Spectracom spectracom: [system] Frequency Error
Mar 16 21:38:44 Spectracom spectracom: [system] STATUS CHANGE.
Mar 16 21:38:44 Spectracom spectracom: [system] ACTIVE ALARMS: MAJOR MINOR
Mar 16 21:38:44 Spectracom spectracom: [system] Antenna Problem
Mar 16 21:38:44 Spectracom spectracom: [system] Frequency Error
Mar 16 21:41:32 Spectracom spectracom: [system] STATUS CHANGE.
Mar 16 21:41:32 Spectracom spectracom: [system] ACTIVE ALARMS: MINOR
Mar 16 21:41:32 Spectracom spectracom: [system] Antenna Problem
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Internet

Figure 3-94: Alarm Log Screen

The Alarm Log (Figure 3-94) is a running list of the alarms (with descriptive information) experienced by the NetClock.

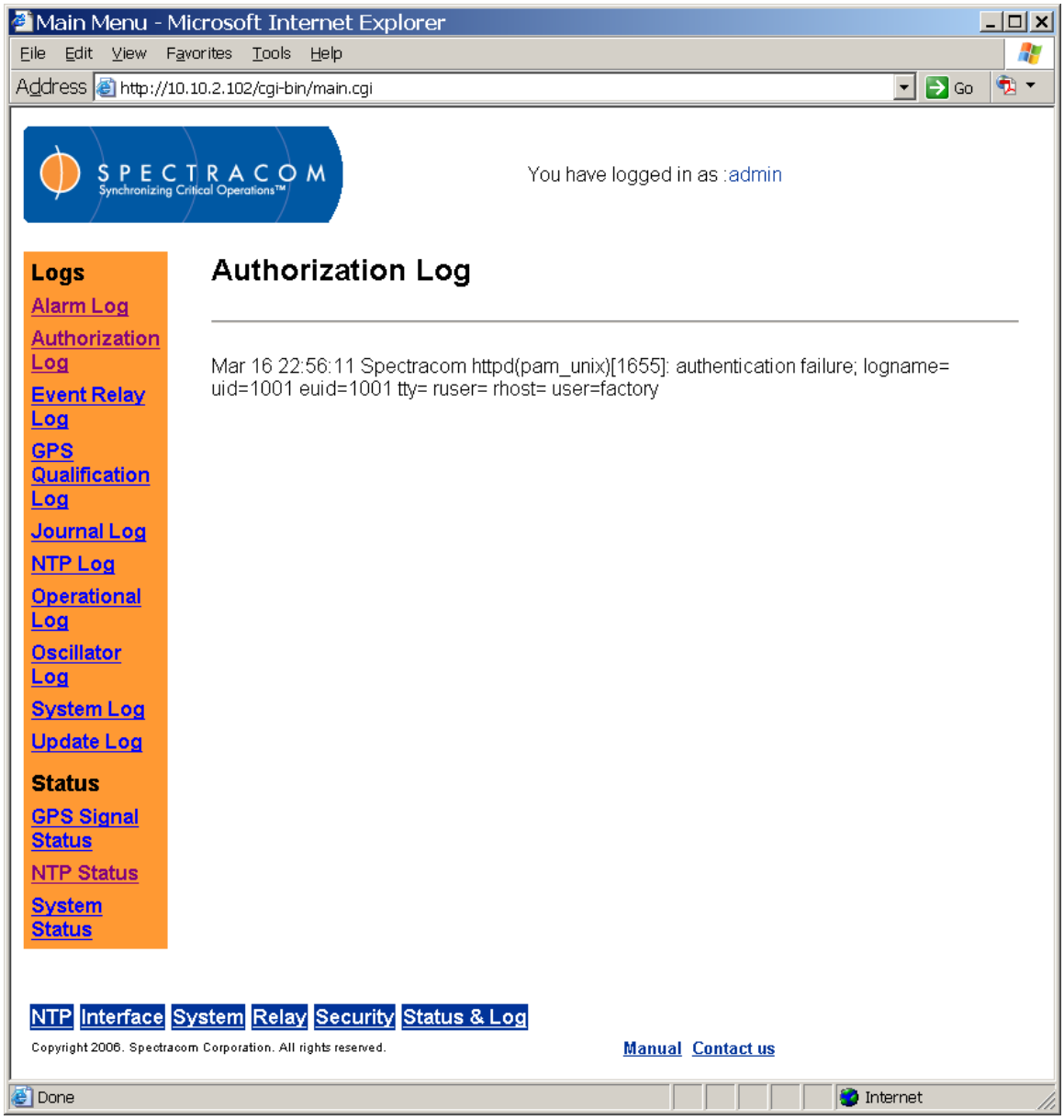


Figure 3-95: Authorization Log Screen

The Authorization Log (Figure 3-95) is a running list of authenticated users who have accessed the NetClock.

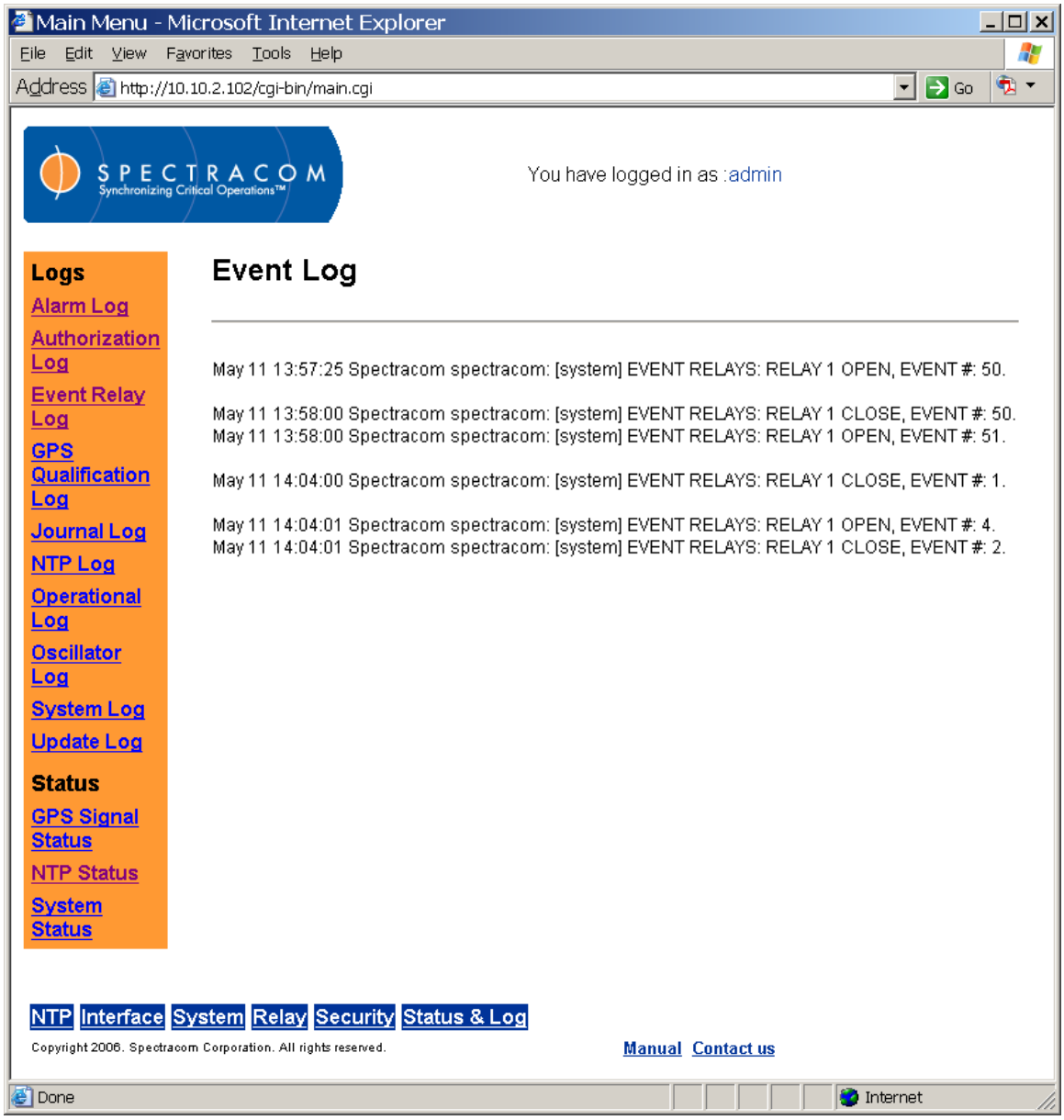

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
Alarm Log
Authorization Log
Event Relay Log
GPS Qualification Log
Journal Log
NTP Log
Operational Log
Oscillator Log
System Log
Update Log
Status
GPS Signal Status
NTP Status
System Status
Event Log
May 11 13:57:25 Spectracom spectracom: [system] EVENT RELAYS: RELAY 1 OPEN, EVENT #: 50.
May 11 13:58:00 Spectracom spectracom: [system] EVENT RELAYS: RELAY 1 CLOSE, EVENT #: 50.
May 11 13:58:00 Spectracom spectracom: [system] EVENT RELAYS: RELAY 1 OPEN, EVENT #: 51.
May 11 14:04:00 Spectracom spectracom: [system] EVENT RELAYS: RELAY 1 CLOSE, EVENT #: 1.
May 11 14:04:01 Spectracom spectracom: [system] EVENT RELAYS: RELAY 1 OPEN, EVENT #: 4.
May 11 14:04:01 Spectracom spectracom: [system] EVENT RELAYS: RELAY 1 CLOSE, EVENT #: 2.
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-96: Event Log Screen

The Event Log (Figure 3-96) is a running list of the event timer relay activity.

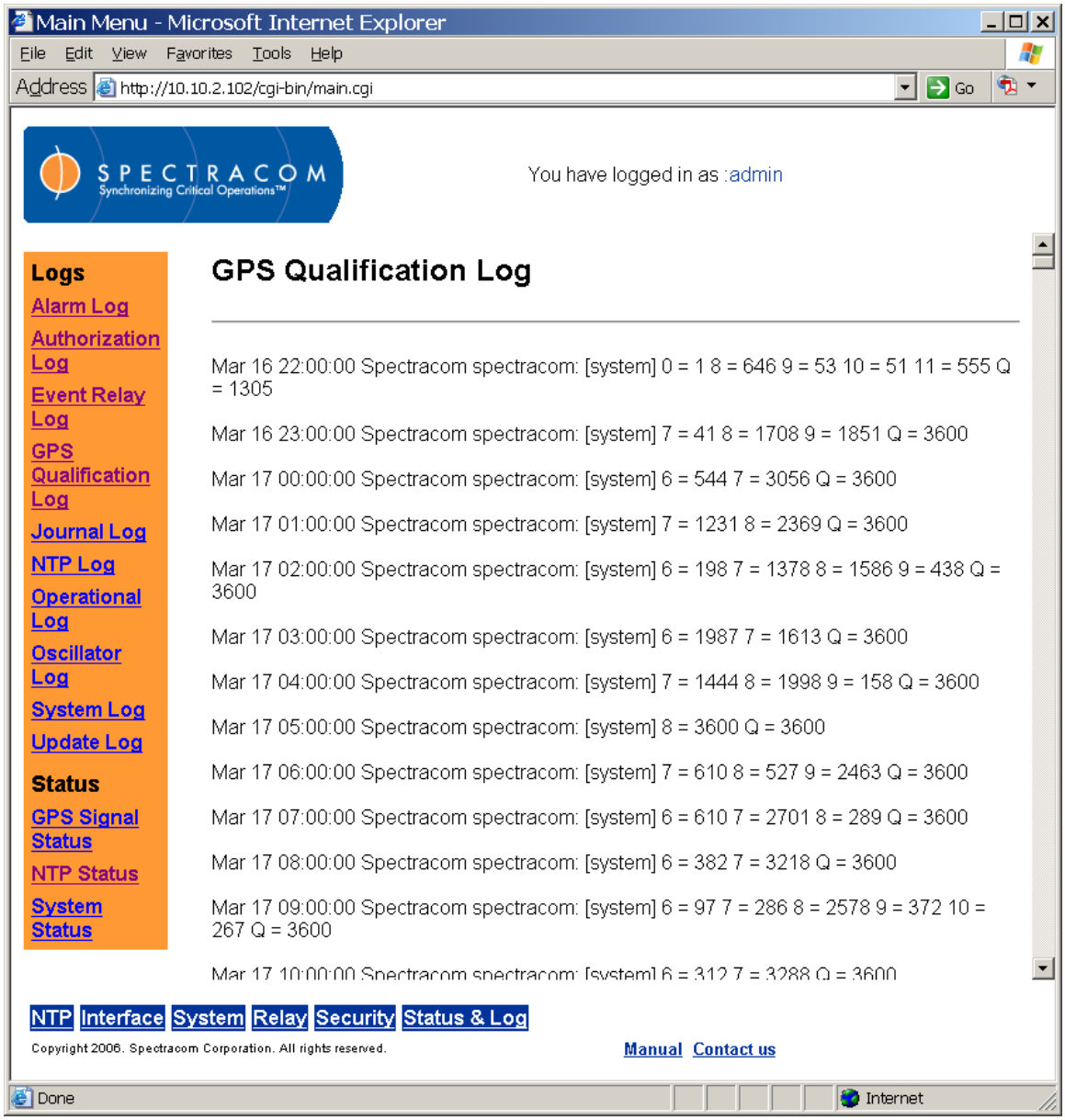

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
Alarm Log
Authorization Log
Event Relay Log
GPS Qualification Log
Journal Log
NTP Log
Operational Log
Oscillator Log
System Log
Update Log
Status
GPS Signal Status
NTP Status
System Status
GPS Qualification Log
Mar 16 22:00:00 Spectracom spectracom: [system] 0 = 1 8 = 646 9 = 53 10 = 51 11 = 555 Q = 1305
Mar 16 23:00:00 Spectracom spectracom: [system] 7 = 41 8 = 1708 9 = 1851 Q = 3600
Mar 17 00:00:00 Spectracom spectracom: [system] 6 = 544 7 = 3056 Q = 3600
Mar 17 01:00:00 Spectracom spectracom: [system] 7 = 1231 8 = 2369 Q = 3600
Mar 17 02:00:00 Spectracom spectracom: [system] 6 = 198 7 = 1378 8 = 1586 9 = 438 Q = 3600
Mar 17 03:00:00 Spectracom spectracom: [system] 6 = 1987 7 = 1613 Q = 3600
Mar 17 04:00:00 Spectracom spectracom: [system] 7 = 1444 8 = 1998 9 = 158 Q = 3600
Mar 17 05:00:00 Spectracom spectracom: [system] 8 = 3600 Q = 3600
Mar 17 06:00:00 Spectracom spectracom: [system] 7 = 610 8 = 527 9 = 2463 Q = 3600
Mar 17 07:00:00 Spectracom spectracom: [system] 6 = 610 7 = 2701 8 = 289 Q = 3600
Mar 17 08:00:00 Spectracom spectracom: [system] 6 = 382 7 = 3218 Q = 3600
Mar 17 09:00:00 Spectracom spectracom: [system] 6 = 97 7 = 286 8 = 2578 9 = 372 10 = 267 Q = 3600
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-97: GPS Qualification Log Screen

The GPS Qualification Log (Figure 3-97) is a running list of the NetClock's GPS satellite signal activity.

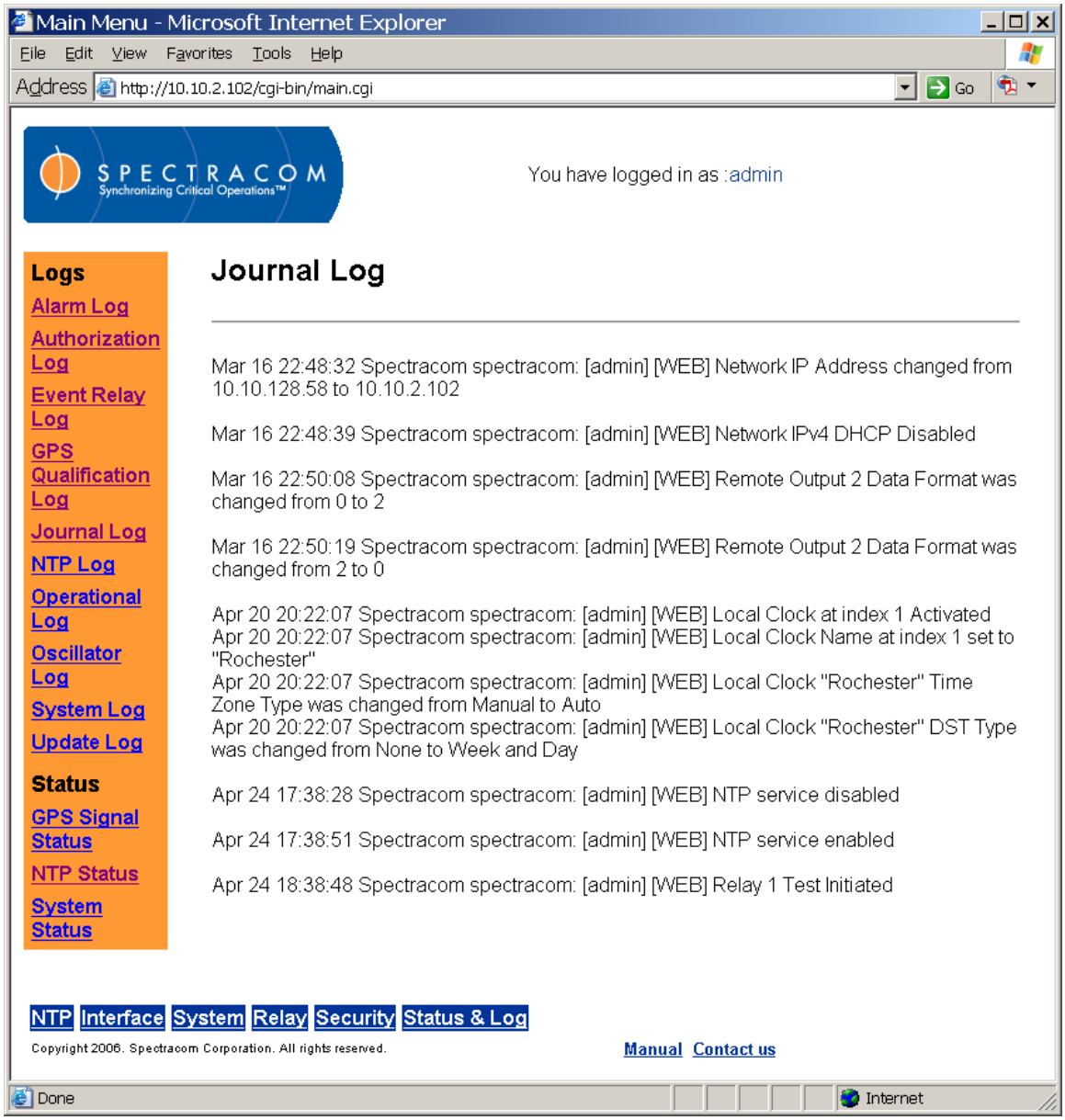

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
Alarm Log
Authorization Log
Event Relay Log
GPS Qualification Log
Journal Log
NTP Log
Operational Log
Oscillator Log
System Log
Update Log
Status
GPS Signal Status
NTP Status
System Status
Journal Log
Mar 16 22:48:32 Spectracom spectracom: [admin] [WEB] Network IP Address changed from 10.10.128.58 to 10.10.2.102
Mar 16 22:48:39 Spectracom spectracom: [admin] [WEB] Network IPv4 DHCP Disabled
Mar 16 22:50:08 Spectracom spectracom: [admin] [WEB] Remote Output 2 Data Format was changed from 0 to 2
Mar 16 22:50:19 Spectracom spectracom: [admin] [WEB] Remote Output 2 Data Format was changed from 2 to 0
Apr 20 20:22:07 Spectracom spectracom: [admin] [WEB] Local Clock at index 1 Activated
Apr 20 20:22:07 Spectracom spectracom: [admin] [WEB] Local Clock Name at index 1 set to "Rochester"
Apr 20 20:22:07 Spectracom spectracom: [admin] [WEB] Local Clock "Rochester" Time Zone Type was changed from Manual to Auto
Apr 20 20:22:07 Spectracom spectracom: [admin] [WEB] Local Clock "Rochester" DST Type was changed from None to Week and Day
Apr 24 17:38:28 Spectracom spectracom: [admin] [WEB] NTP service disabled
Apr 24 17:38:51 Spectracom spectracom: [admin] [WEB] NTP service enabled
Apr 24 18:38:48 Spectracom spectracom: [admin] [WEB] Relay 1 Test Initiated
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-98: Journal Log Screen

Whenever a user changes the NetClock's configuration, the change (who performed it and what the change was) is recorded in the Journal Log (Figure 3-98).

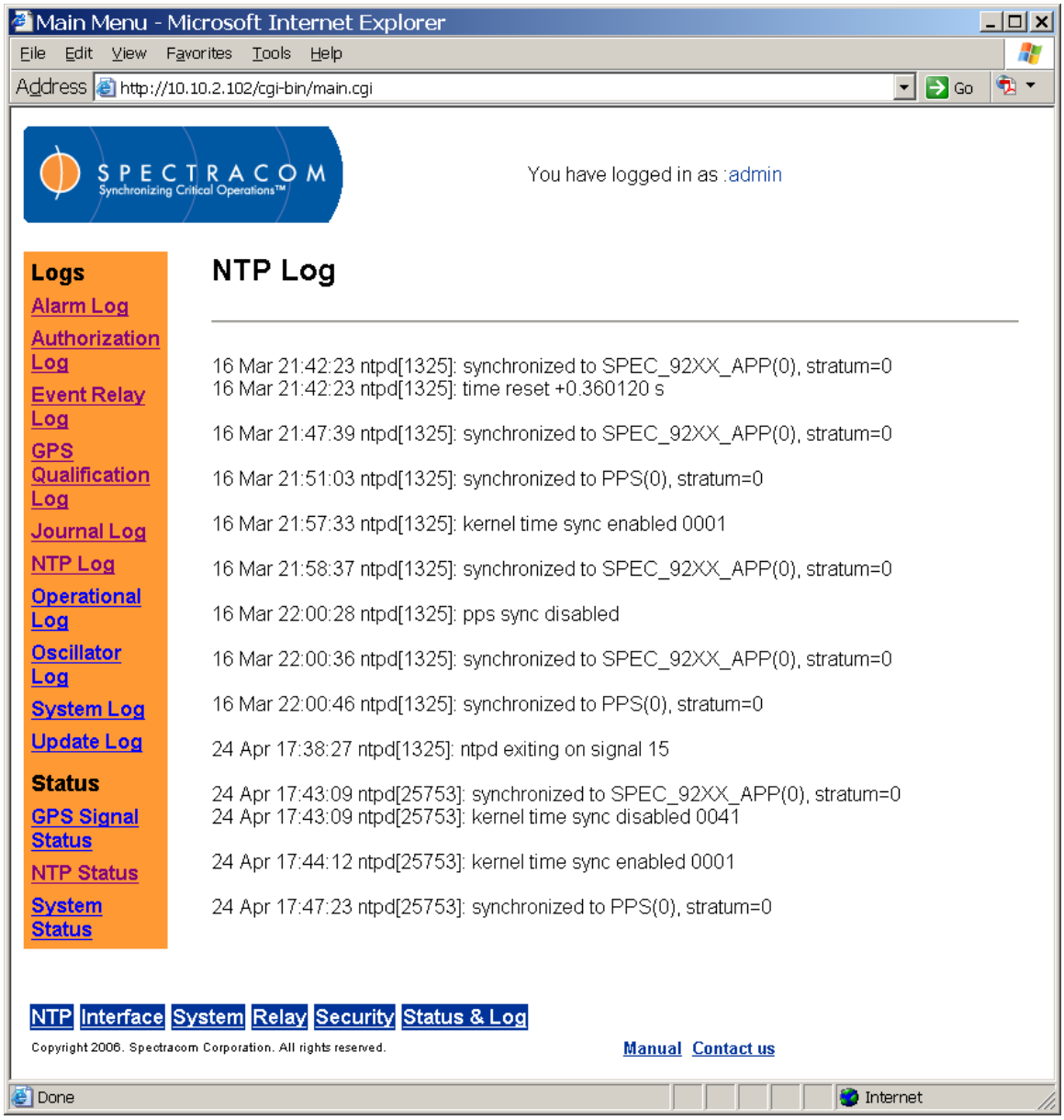

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
Alarm Log
Authorization Log
Event Relay Log
GPS Qualification Log
Journal Log
NTP Log
Operational Log
Oscillator Log
System Log
Update Log
Status
GPS Signal Status
NTP Status
System Status
NTP Log
16 Mar 21:42:23 ntpd[1325]: synchronized to SPEC_92XX_APP(0), stratum=0
16 Mar 21:42:23 ntpd[1325]: time reset +0.360120 s
16 Mar 21:47:39 ntpd[1325]: synchronized to SPEC_92XX_APP(0), stratum=0
16 Mar 21:51:03 ntpd[1325]: synchronized to PPS(0), stratum=0
16 Mar 21:57:33 ntpd[1325]: kernel time sync enabled 0001
16 Mar 21:58:37 ntpd[1325]: synchronized to SPEC_92XX_APP(0), stratum=0
16 Mar 22:00:28 ntpd[1325]: pps sync disabled
16 Mar 22:00:36 ntpd[1325]: synchronized to SPEC_92XX_APP(0), stratum=0
16 Mar 22:00:46 ntpd[1325]: synchronized to PPS(0), stratum=0
24 Apr 17:38:27 ntpd[1325]: ntpd exiting on signal 15
24 Apr 17:43:09 ntpd[25753]: synchronized to SPEC_92XX_APP(0), stratum=0
24 Apr 17:43:09 ntpd[25753]: kernel time sync disabled 0041
24 Apr 17:44:12 ntpd[25753]: kernel time sync enabled 0001
24 Apr 17:47:23 ntpd[25753]: synchronized to PPS(0), stratum=0
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-99: NTP Log Screen

The NTP Log (Figure 3-99) is a running list of NTP activity on the NetClock.

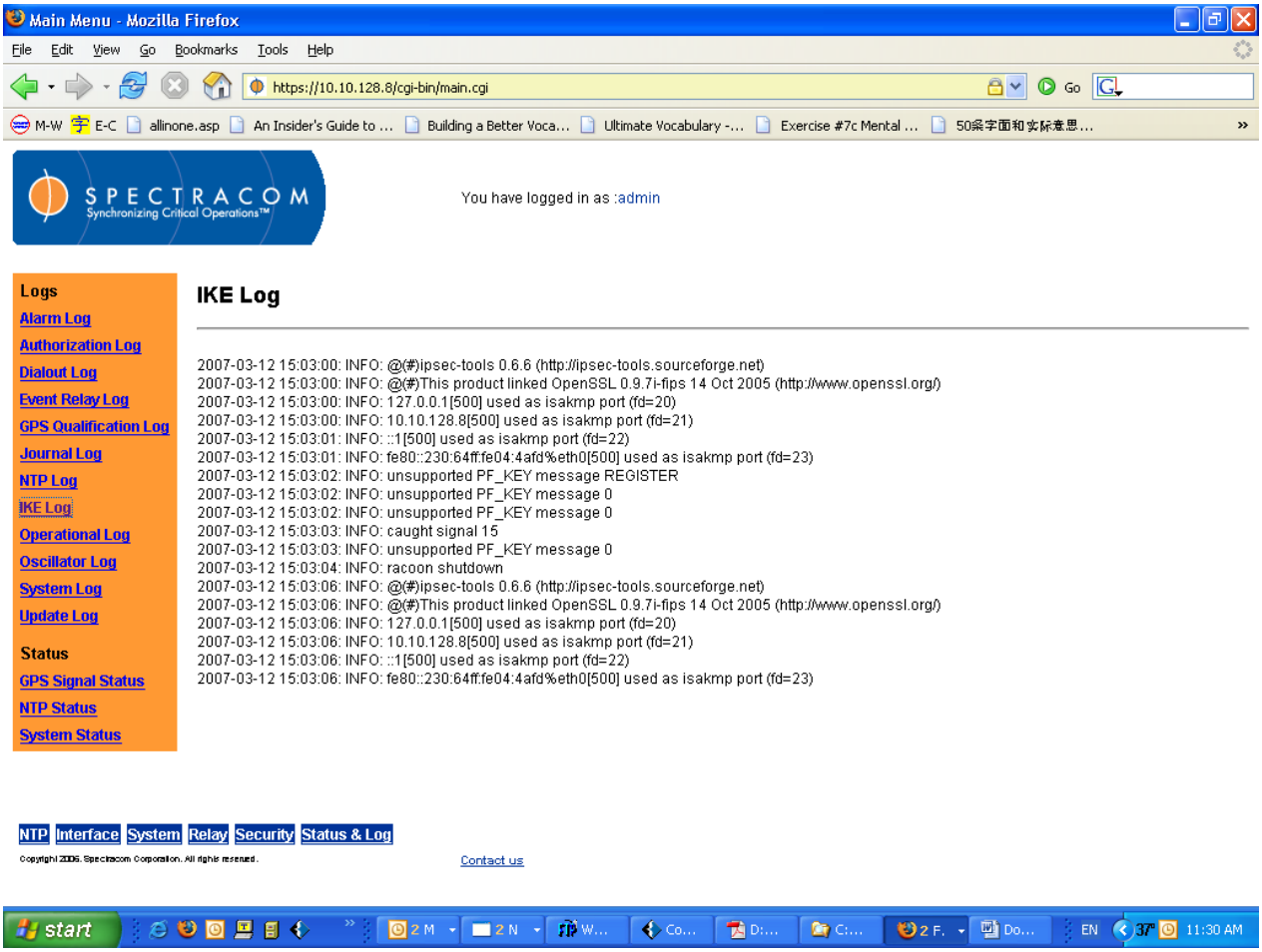

Main Menu - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://10.10.128.8/cgi-bin/main.cgi
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
Alarm Log
Authorization Log
Dialout Log
Event Relay Log
GPS Qualification Log
Journal Log
NTP Log
IKE Log
Operational Log
Oscillator Log
System Log
Update Log
Status
GPS Signal Status
NTP Status
System Status
IKE Log
2007-03-12 15:03:00: INFO: @(#)ipsec-tools 0.6.6 (http://ipsec-tools.sourceforge.net)
2007-03-12 15:03:00: INFO: @(#)This product linked OpenSSL 0.9.7i-fips 14 Oct 2005 (http://www.openssl.org/)
2007-03-12 15:03:00: INFO: 127.0.0.1[500] used as isakmp port (fd=20)
2007-03-12 15:03:00: INFO: 10.10.128.8[500] used as isakmp port (fd=21)
2007-03-12 15:03:01: INFO: ::1[500] used as isakmp port (fd=22)
2007-03-12 15:03:01: INFO: fe80::230:64ff:fe04:4afd%eth0[500] used as isakmp port (fd=23)
2007-03-12 15:03:02: INFO: unsupported PF_KEY message REGISTER
2007-03-12 15:03:02: INFO: unsupported PF_KEY message 0
2007-03-12 15:03:02: INFO: unsupported PF_KEY message 0
2007-03-12 15:03:03: INFO: caught signal 15
2007-03-12 15:03:03: INFO: unsupported PF_KEY message 0
2007-03-12 15:03:04: INFO: racoon shutdown
2007-03-12 15:03:06: INFO: @(#)ipsec-tools 0.6.6 (http://ipsec-tools.sourceforge.net)
2007-03-12 15:03:06: INFO: @(#)This product linked OpenSSL 0.9.7i-fips 14 Oct 2005 (http://www.openssl.org/)
2007-03-12 15:03:06: INFO: 127.0.0.1[500] used as isakmp port (fd=20)
2007-03-12 15:03:06: INFO: 10.10.128.8[500] used as isakmp port (fd=21)
2007-03-12 15:03:06: INFO: ::1[500] used as isakmp port (fd=22)
2007-03-12 15:03:06: INFO: fe80::230:64ff:fe04:4afd%eth0[500] used as isakmp port (fd=23)
NTP Interface System Relay Security Status & Log
Contact us
start
11:30 AM

Figure 3-100: IKE Log Screen

The IKE Log (Figure 3-100) is useful for troubleshooting the status of the IPSec IKE SA configuration.

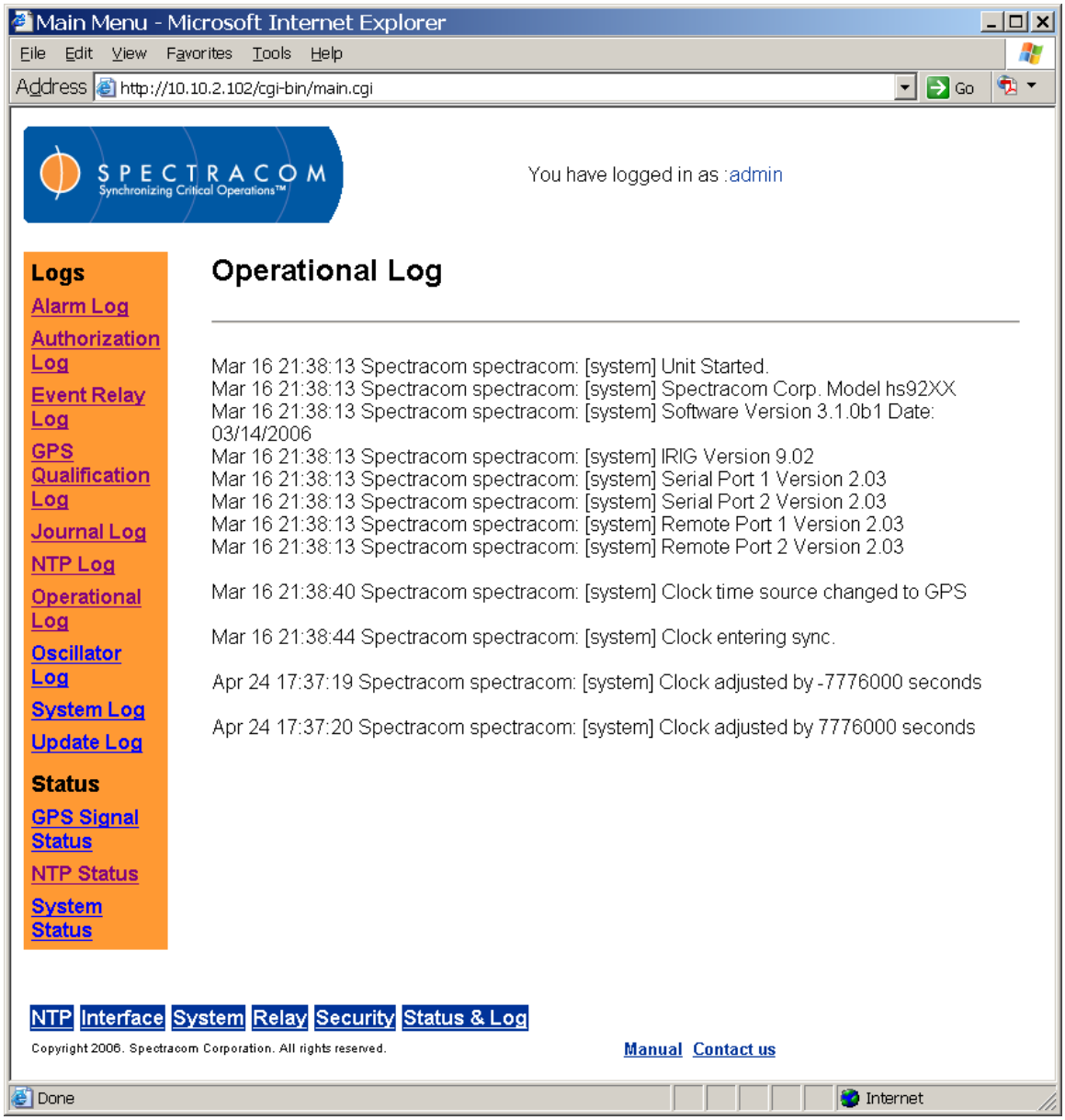

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
Alarm Log
Authorization Log
Event Relay Log
GPS Qualification Log
Journal Log
NTP Log
Operational Log
Oscillator Log
System Log
Update Log
Status
GPS Signal Status
NTP Status
System Status
Operational Log
Mar 16 21:38:13 Spectracom spectracom: [system] Unit Started.
Mar 16 21:38:13 Spectracom spectracom: [system] Spectracom Corp. Model hs92XX
Mar 16 21:38:13 Spectracom spectracom: [system] Software Version 3.1.0b1 Date: 03/14/2006
Mar 16 21:38:13 Spectracom spectracom: [system] IRIG Version 9.02
Mar 16 21:38:13 Spectracom spectracom: [system] Serial Port 1 Version 2.03
Mar 16 21:38:13 Spectracom spectracom: [system] Serial Port 2 Version 2.03
Mar 16 21:38:13 Spectracom spectracom: [system] Remote Port 1 Version 2.03
Mar 16 21:38:13 Spectracom spectracom: [system] Remote Port 2 Version 2.03
Mar 16 21:38:40 Spectracom spectracom: [system] Clock time source changed to GPS
Mar 16 21:38:44 Spectracom spectracom: [system] Clock entering sync.
Apr 24 17:37:19 Spectracom spectracom: [system] Clock adjusted by -7776000 seconds
Apr 24 17:37:20 Spectracom spectracom: [system] Clock adjusted by 7776000 seconds
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-101: Operational Log Screen

The Operational Log (Figure 3-101) is a running list of NetClock operations, such as system updates and clock synchronizations.

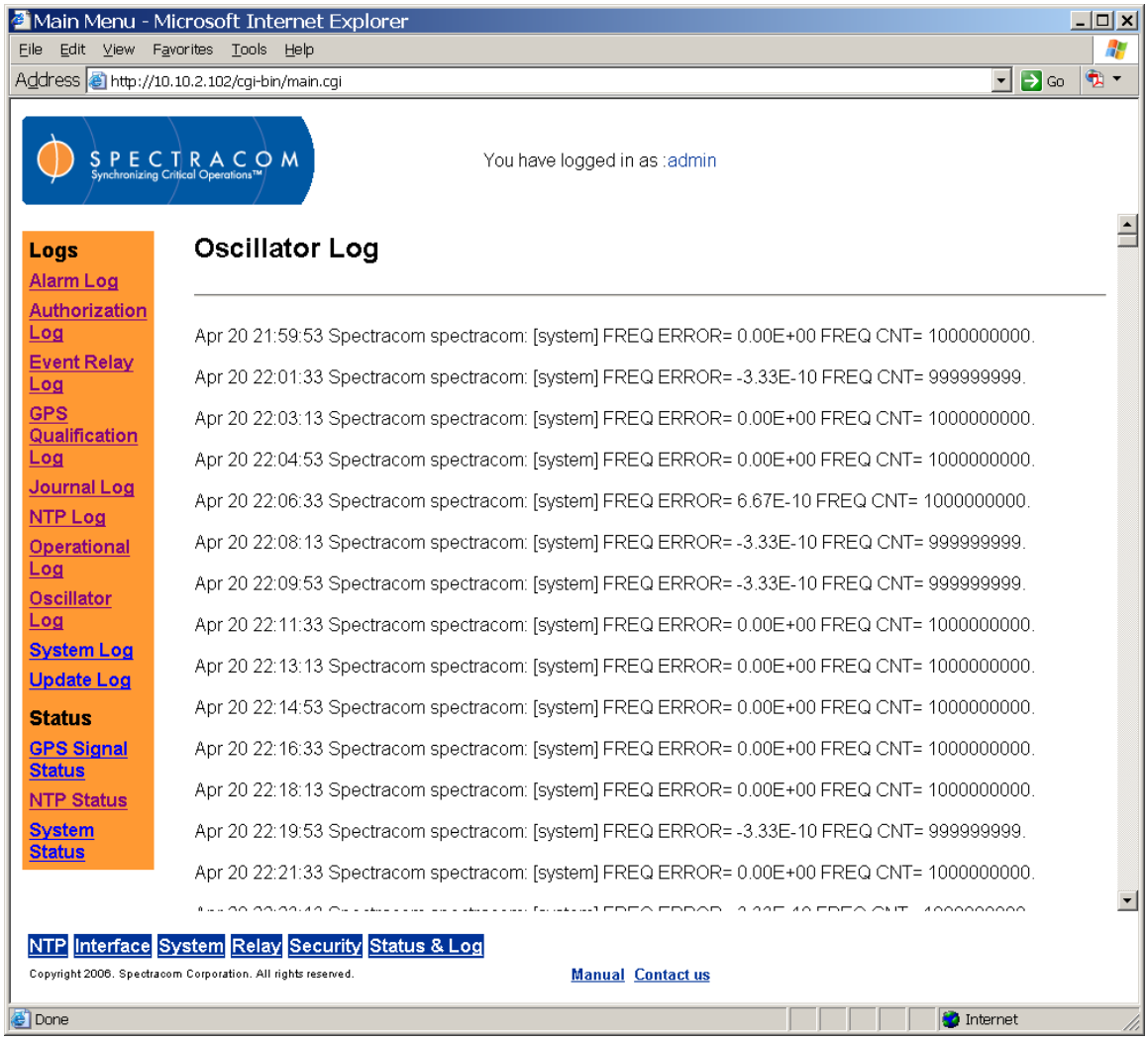

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
Alarm Log
Authorization Log
Event Relay Log
GPS Qualification Log
Journal Log
NTP Log
Operational Log
Oscillator Log
System Log
Update Log
Status
GPS Signal Status
NTP Status
System Status
Oscillator Log
Apr 20 21:59:53 Spectracom spectracom: [system] FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000.
Apr 20 22:01:33 Spectracom spectracom: [system] FREQ ERROR= -3.33E-10 FREQ CNT= 999999999.
Apr 20 22:03:13 Spectracom spectracom: [system] FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000.
Apr 20 22:04:53 Spectracom spectracom: [system] FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000.
Apr 20 22:06:33 Spectracom spectracom: [system] FREQ ERROR= 6.67E-10 FREQ CNT= 1000000000.
Apr 20 22:08:13 Spectracom spectracom: [system] FREQ ERROR= -3.33E-10 FREQ CNT= 999999999.
Apr 20 22:09:53 Spectracom spectracom: [system] FREQ ERROR= -3.33E-10 FREQ CNT= 999999999.
Apr 20 22:11:33 Spectracom spectracom: [system] FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000.
Apr 20 22:13:13 Spectracom spectracom: [system] FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000.
Apr 20 22:14:53 Spectracom spectracom: [system] FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000.
Apr 20 22:16:33 Spectracom spectracom: [system] FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000.
Apr 20 22:18:13 Spectracom spectracom: [system] FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000.
Apr 20 22:19:53 Spectracom spectracom: [system] FREQ ERROR= -3.33E-10 FREQ CNT= 999999999.
Apr 20 22:21:33 Spectracom spectracom: [system] FREQ ERROR= 0.00E+00 FREQ CNT= 1000000000.
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-102: Oscillator Log Screen

The Oscillator Log (Figure 3-102) is a running list of the NetClock's oscillator activity.

NOTE: The notation FREQ ERROR is a normal entry in the log. It is not a frequency alarm condition and does not indicate a problem with the unit.

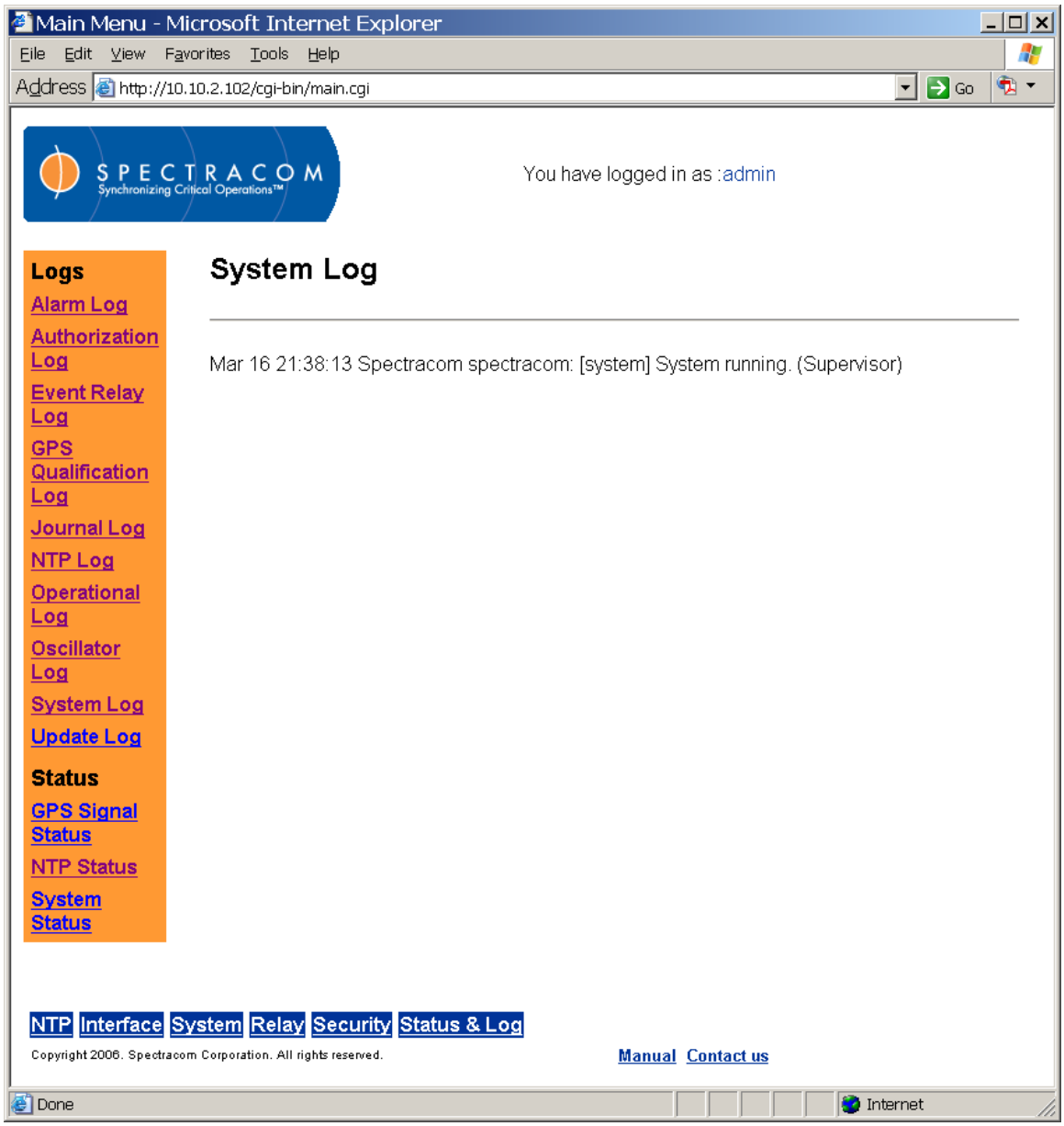


Figure 3-103: System Log Screen

The System Log (Figure 3-103) is a running list of system information and status messages that may be used by factory personnel for troubleshooting. This log records internal system information that is not intended for customer use.

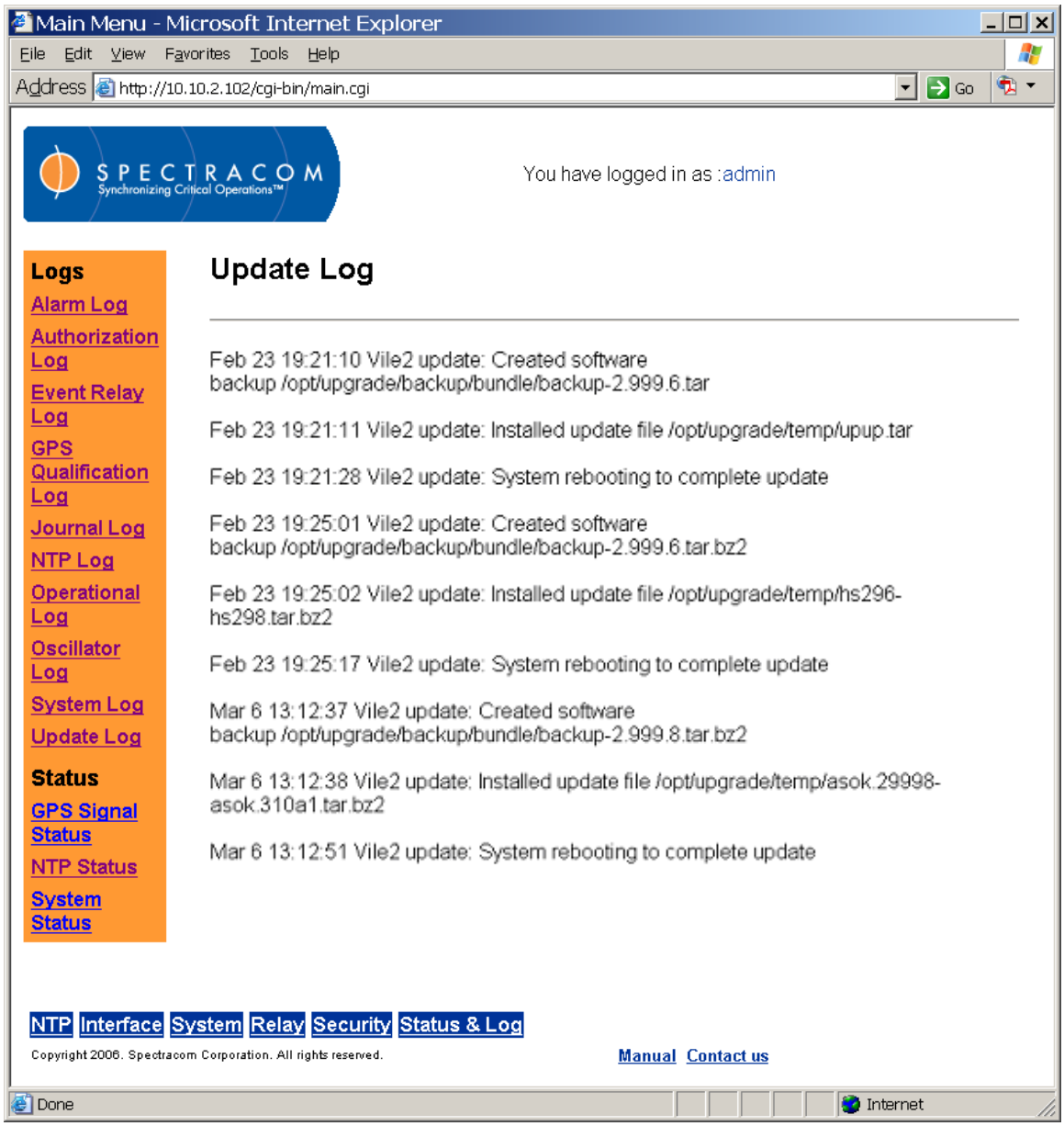

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.10.2.102/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
Alarm Log
Authorization Log
Event Relay Log
GPS Qualification Log
Journal Log
NTP Log
Operational Log
Oscillator Log
System Log
Update Log
Status
GPS Signal Status
NTP Status
System Status
Update Log
Feb 23 19:21:10 Vile2 update: Created software backup /opt/upgrade/backup/bundle/backup-2.999.6.tar
Feb 23 19:21:11 Vile2 update: Installed update file /opt/upgrade/temp/upup.tar
Feb 23 19:21:28 Vile2 update: System rebooting to complete update
Feb 23 19:25:01 Vile2 update: Created software backup /opt/upgrade/backup/bundle/backup-2.999.6.tar.bz2
Feb 23 19:25:02 Vile2 update: Installed update file /opt/upgrade/temp/hs296-hs298.tar.bz2
Feb 23 19:25:17 Vile2 update: System rebooting to complete update
Mar 6 13:12:37 Vile2 update: Created software backup /opt/upgrade/backup/bundle/backup-2.999.8.tar.bz2
Mar 6 13:12:38 Vile2 update: Installed update file /opt/upgrade/temp/asok.29998-asok.310a1.tar.bz2
Mar 6 13:12:51 Vile2 update: System rebooting to complete update
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 3-104: Update Log Screen

The Update Log (Figure 3-104) is a running list of software updates performed on the NetClock. Software updates are performed using a utility program provided by Spectracom.

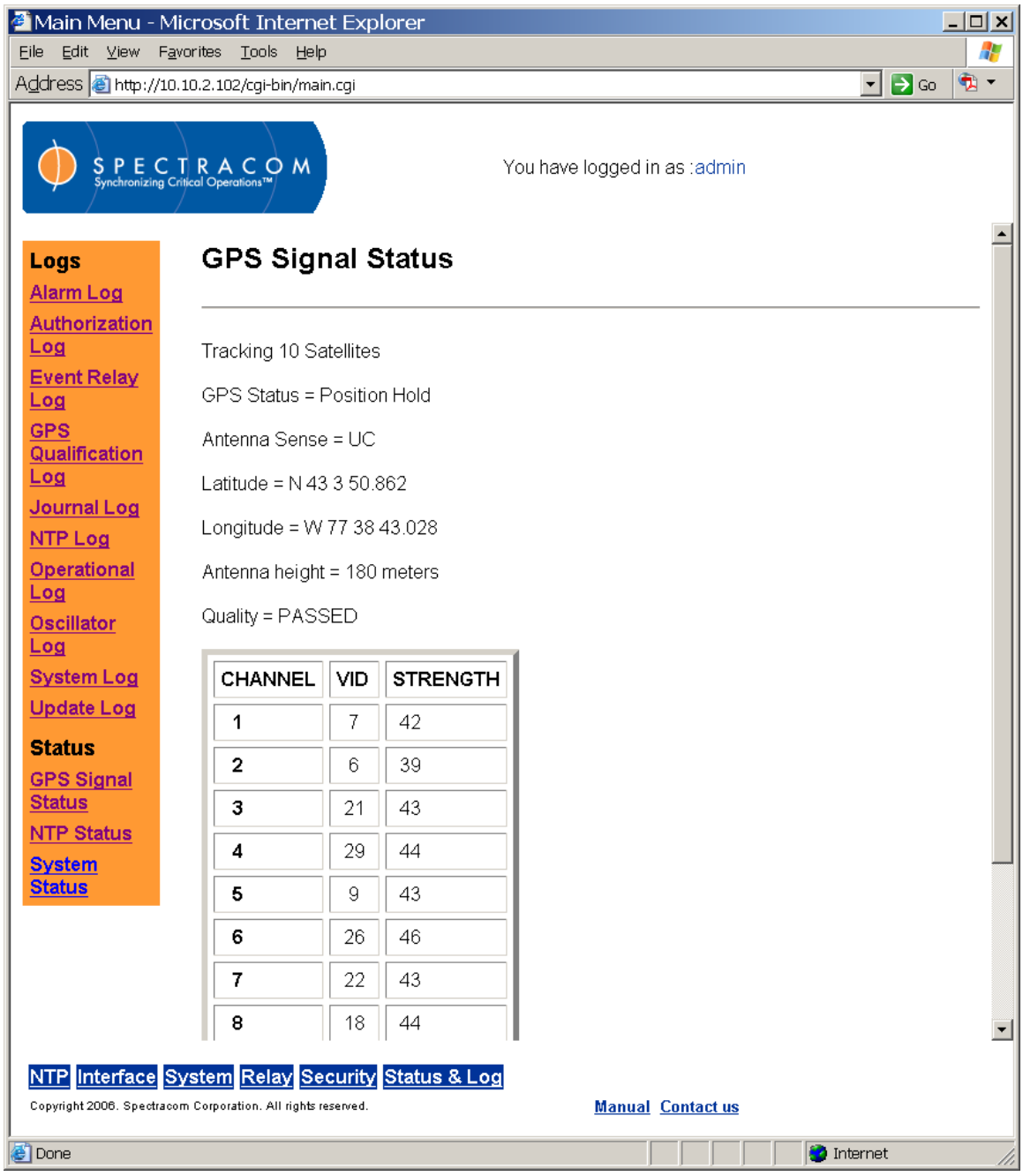


Figure 3-105: GPS Signal Status Screen

The GPS Signal Status screen (Figure 3-105) provides insight into the GPS receiver's operation and the signal quality from the satellites. This information is useful to verify proper antenna placement and receiver performance during installation and later troubleshooting. The page describes the number of satellites being tracked and will indicate that the NetClock is "acquiring" if it is still searching for qualified satellites. "Bad Geometry" means the number or position of satellites being tracked is not sufficient to calculate position. A "2D Fix" means the receiver is tracking at least three qualified satellites, while a "4D Fix" means the receiver is tracking at least four satellites. "Position Hold" means the GPS receiver has collected enough information to

determine its location. Some other terms you will encounter on the GPS Signal Status screen include:

Antenna Sense = SSSSS
SSSSS reports the status of the antenna sense circuit. There are three main flags (OK, Over Current, and Under Current). The three flags are described here:

OK Flag
The OK flag is displayed if both antenna sense bits are cleared. This indicates that the antenna is drawing current within the normal range.

Over Current Flag
This flag is displayed if the over current bit is set. This indicates that too much current is being drawn through the circuit and the overload protection circuit is limiting the feed current. The receiver will attempt to continue the normal acquisition and tracking process regardless of the antenna status.

Under Current Flag
This flag is displayed if the undercurrent bit is set. This indicates that little or no current is being drawn through the circuit, which may be due to a disconnected antenna, a severed antenna cable or a damaged antenna. The receiver will attempt to continue the normal acquisition and tracking process regardless of the antenna status.

Undercurrent indication < 8 mA
Overcurrent indication > 80 mA

NOTE: This condition will also be present if a GPS antenna splitter that does not contain a load to simulate an antenna being present is being used.

Latitude = [N:S][DD MM SS.SSSS]
Longitude = [E:W][DDD MM SS.SSSS]
Where: N = North latitude
S = South Latitude
E = East Longitude
W = West Longitude
D = Degree
M = Minute
S = Second

Quality = QQQQQ
QQQQQ = Result of GPS qualification, either PASSED or FAILED. The GPS signal is considered qualified when at least one satellite is received having a vehicle ID of at least 4 that are available for Position Fix Usage while in the normal mode of operation (Or at least 1 satellite that is available for position fix when the unit is single satellite mode).

Information on each satellite the receiver is currently tracking is presented in table form. The table columns are described below:

CHANNEL = Channel Number of the GPS receiver, 1…12

VID = Vehicle (satellite) Identification Number, 1…37

STRENGTH = Signal strength value relative to the Signal to Noise Ratio [SNR]. Range: 0…255, the higher the number, the greater the receiver signal.

NOTE: The NTP Status screen (Figure 3-106) is discussed in the *Configuring NTP* section of this manual.

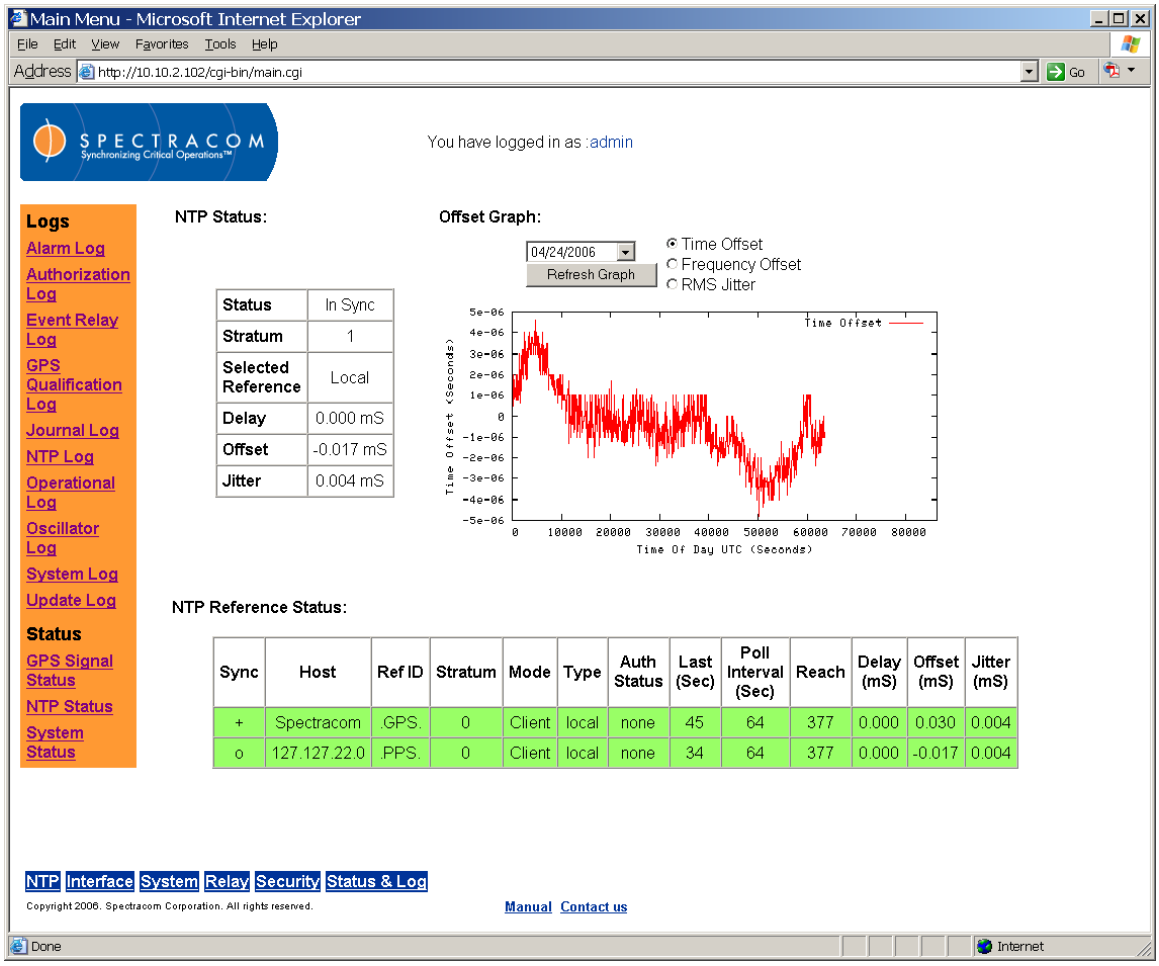


Figure 3-106: NTP Status Screen

The System Status screen (Figure 3-107) consists of four sections that provide the user with the software revision levels, the current time synchronization status, the results of internal unit testing, and the features and options that are currently enabled and disabled.

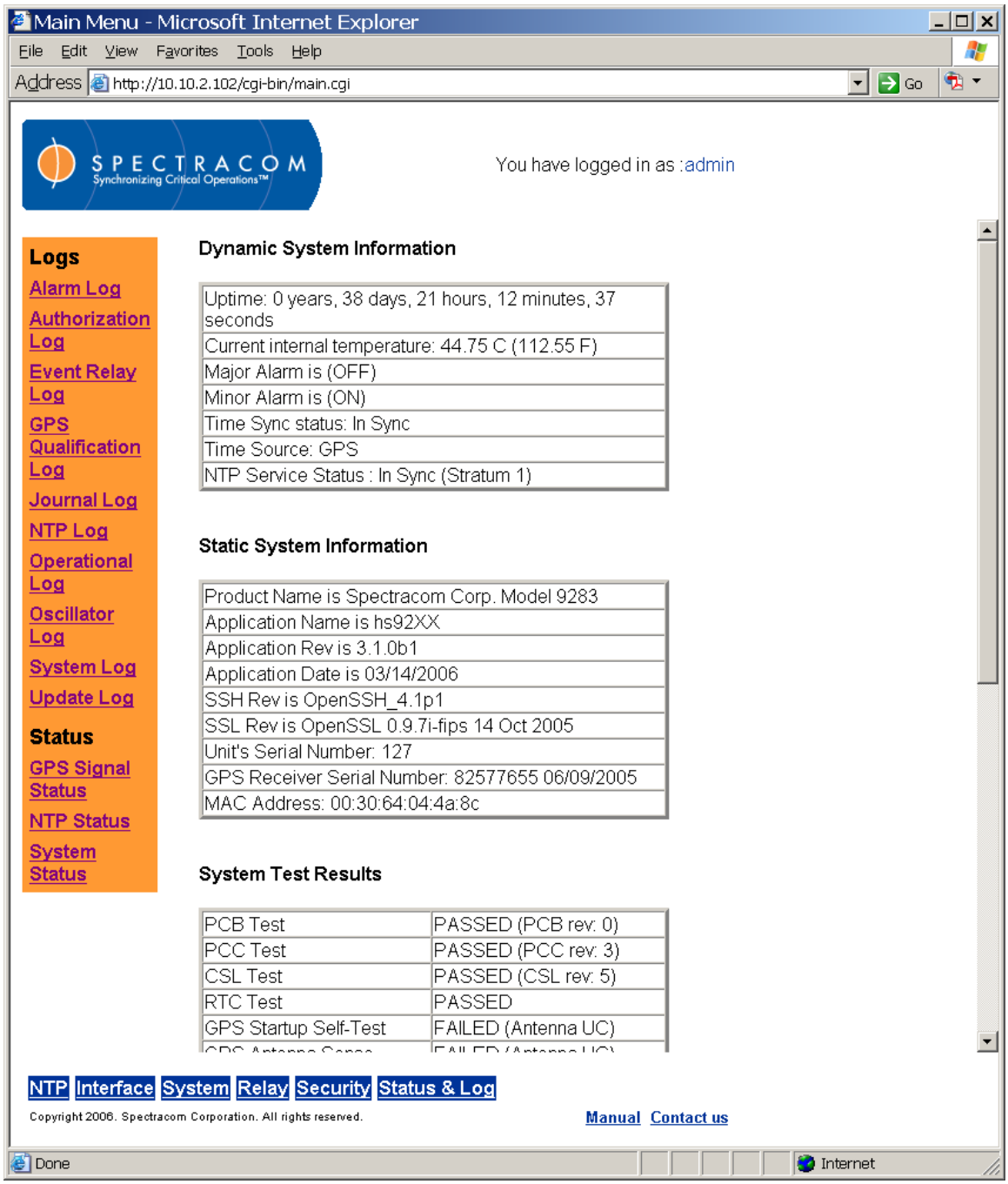


Figure 3-107: System Status Screen (1 of 2)

The **Dynamic System Information** section contains the elapsed time that the unit has been powered-up for, the internal temperature of the unit, the status of the major and minor alarms, the current time synchronization status and the current external reference identifier.

Time Source – The time source field contains the current source for time input. The possible inputs are as follows:

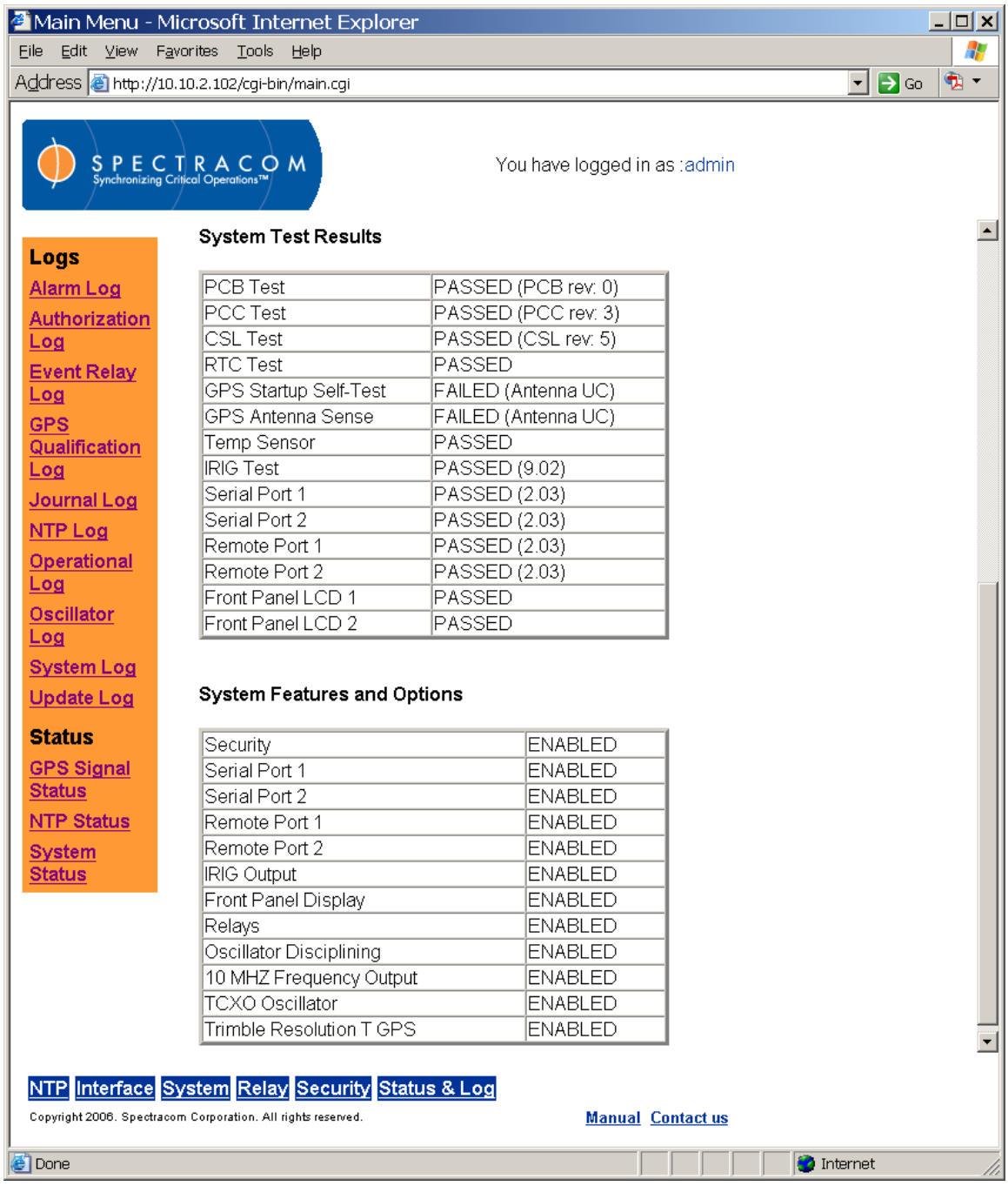


Figure 3-108: System Status Screen (2 of 2)

None – No Time Source has been found after startup.

GPS – The GPS receiver is the Primary Time Source for the Models 9383 and 9189.

Modem – When Option 03 is installed, the Modem maybe used as a Primary Time Source or Secondary (backup) Time Source to GPS for the 9300 Series.

User – The Time Source is the result of the user setting the time from the System Setup/System Time web browser user interface page when no Time Source is present.

The **Static System Information** section of the System Status screen provides the software revisions, the NetClock's Serial Number, and the MAC address.

The **System Test Results** section contains the results of the internal tests that are run. These test are not complete checks of the entire paths (For example, the Serial port may pass even though it has been damaged by a surge).

GPS Startup Self-Test – The GPS Startup Self-Test will indicate the status of the antenna, antenna cable and the GPS receiver at the time of power-up only. If the antenna cable was not connected, shorted or open at the time of power-up, and/or if there is a problem with the GPS receiver or antenna or both at the time of power-up, this test will indicate FAILED. "Antenna UC" means the antenna was not connected and "Antenna OC" indicates there was a short in the cable at the time of power-up. "Antenna NV" means an unknown antenna problem existed at power-up. "GPS & Antenna" means that both GPS receiver and Antenna problems were detected at power-up.

GPS Antenna Sense – The GPS Antenna Sense is a current status of the antenna, antenna cable and the GPS receiver. If the antenna cable is currently not connected, shorted or open, and/or if there is a problem with the GPS receiver or antenna or both, this test will indicate FAILED. "Antenna UC" means the antenna is not currently connected and "Antenna OC" indicates a short in the cable. "Antenna NV" means an unknown antenna problem. "GPS & Antenna" means that both GPS receiver and Antenna problems were detected.

Modem Test (Applicable only to units with Option 03 installed) – The Modem Test will indicate "Console Mode" if the Serial Setup Interface is set to Console mode instead of Client mode. This indicates that the modem is not currently being used. If the modem feature is desired, in the modem configuration page, change the mode to Client Mode.

When the NetClock initially boots up, the mode is set to Serial Setup Interface. When the mode is set to Modem and before every modem dial-out call, the modem is sent a command. If the unit gets a response from the modem, the field is set to PASSED. If the unit gets no response or a bad response from the modem, then the field is set to FAILED and the reason is indicated as shown below:
Reasons:

Not Found – There is no modem connected, the modem is incorrectly connected, or it is not turned on.

Modem Error – The modem gave a response indicating an unspecified problem.

The **System Features and Options** section provides the current status of all the features and options that are available for your particular NetClock. Features that are currently turned on will indicate "ENABLED". Features that indicate "DISABLED" are not enabled. However, the disabled features may be "enabled" after the original purchase. If an option, which is enabled, fails to correctly initialize and become ready to be used its status is **ERROR**.

Option 03 can be enabled in the field (Options 04 and 05 must be purchased with the unit when it is initially ordered). With the future purchase of the Modem option (Option 03), we will provide

a “key hash” that will enable the feature to be turned on. Please contact our Sales department to purchase the option.

The purchase price of the modem option includes the cost for the modem as well as the key to enable the feature. The modem selection is very limited in compatibility. Not all available modems are compatible with the 9300 Series (Must be configured as Hayes AT) so we will supply you with a modem when the option is purchased. If the modem option was not initially purchased, contact our Sales department to purchase the modem option. Refer to *Options* for more information.

4 Day-to-Day Operation

Operation of the 9300 series NetClock is relatively intuitive and requires little operator intervention during normal network activities.

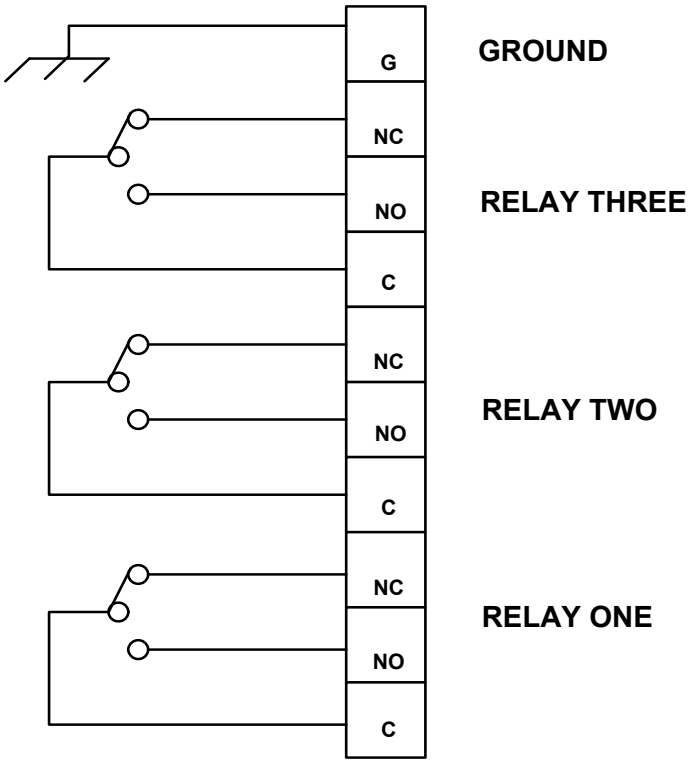
4.1.1 Event and Alarm Relay Outputs

The NetClock features three programmable relay outputs. The relays can be configured as major alarms, minor alarms, or events. They can control bells, whistles, sirens or other devices based on the event/alarm setup. Each event has an assigned start and stop time. An event can be scheduled for daily, monthly, or specific date occurrences.

An example of a daily event schedule is to sound the siren at the fire station at noon every day for five seconds. An example of a dated event is to schedule a test of the emergency evacuation horns on May 9th, 2007 from 10:00 AM to 10:05 AM.

The event timer is configured using the Web UI. Relays are configurable as events or alarm outputs. Refer to the appropriate configuration screens in Section 3 of this manual.

Event and alarm relay contacts are rated at 2.0 Amps, 30 VDC. The relays will be in the de-energized state (refer to Figure 4-1) when power is removed, when a major alarm is present and the relay is configured as a major alarm, or when an event is “on” and the relay is configured as an event output. The relay contacts can be referenced to ground by connecting to Pin G of the Alarm Outputs connector.



NOTE: Relays are shown in the de-energized state (event “off”).

Figure 4-1: Event and Alarm Relay Contacts

4.2 Leap Second occurrence

4.2.1 Reasons for a Leap Second Correction

A **Leap Second** is an intercalary, one-second adjustment that keeps broadcast standards for time of day close to mean solar time. Leap seconds are necessary to keep time standards synchronized with civil calendars, the basis of which is astronomical. They are used to keep the earth's rotation in sync with the UTC time.

If it has been determined by the International Earth Rotation and Reference Systems Service (IERS) that a Leap Second needs to applied, this time correction occurs only at the end of a UTC month, and has only ever been inserted at the end of June 30 or December 31. A Leap Second may be either added or removed, but in the past, the leap seconds have always been added because the earth's rotation is slowing down.

Historically, Leap seconds have been inserted about every 18 months. However, the Earth's rotation rate is unpredictable in the long term, so it is not possible to predict the need for them more than six months in advance.

The NetClock can be alerted of impending leap seconds by either of the following methods:

1. GPS Receiver – The GPS satellite system transmits information regarding a Leap second adjustment at a specific Time and Date an arbitrary number of months in advance.
2. Modem – (Applicable to only units with Option 03 Modem installed). During a modem dial-out call, the call service indicates that a Leap second adjustment at the end of this current calendar month will occur.

4.2.2 Leap Second Alert Notification

The NetClock will announce a pending Leap Second adjustment by the following methods:

1. Data Formats 2 and 7 on the Serial and Remote Ports contain a Leap Second indicator. During the entire calendar month preceding a Leap Second adjustment, these Formats indicate that at the end of the current month a Leap Second Adjustment will be made by having a 'L' rather than a ' ' (space) character in the data stream. Note that his does not indicate the direction of the adjustment as adding or removing seconds. These formats always assume that the Leap Second will be added, not removed.
2. NTP Packets contain two Leap Indicator Bits. In the 24 hours preceding a Leap Second Adjustment, the Leap Indicator Bits (2 bits) which normally are 00b for sync are 01b (1) for Add a Leap Second and 10b (2) for remove a Leap Second. The bit pattern 11b (3) indicates out of sync and in this condition NTP does NOT indicate Leap seconds. The Sync state indicates leap seconds by indicating sync can be 00b, 01b, or 02b.

NOTE: It is the responsibility of the client software utilizing either the Data Formats or NTP time stamps to correct for a Leap Second occurrence. The NetClock will make the correction at the right time. However, because computers and other systems may not utilize the time every second, the Leap second correction may be delayed until the next scheduled interval, unless the software properly handles the advance notice of a pending Leap Second and applies the correction at the right time.

3. The Dynamic System Information box in the “System Status” page located under the web page of “Status and Logs” will display a Leap Second Status box indicating +1 or -1 Leap second adjustment at the end of the month to users during the entire calendar month preceding the actual adjustment.

4.2.3 Sequence of a Leap Second Correction Being Applied

1. The following is the time output sequence that the 9300 Series will utilize to apply the Leap second at UTC midnight (Not local time midnight. The Local time at which the adjustment is made will depend on which Time Zone you are located in).

   A) Sequence of seconds output when adding a leap second:

   56, 57, 58, 59, 60, 0, 1, 2, 3, …

   B) Sequence of seconds output when removing Leap seconds:

   56, 57, 58, 0, 1, 2, 3, 4, …

2. An entry will be made in the Operational log that the time was adjusted for a Leap Second.
   A) An example log entry for a Positive Leap Second is as follows:

   TIME= 23:59:59 DATE= 2005-12-31
   System Clock Service
   Leap second inserted at end of month.

   B) An example log entry for a Negative Leap Second is as follows:

   TIME= 23:59:59 DATE= 2005-12-31
   System Clock Service
   Leap second removed at end of month.

5 Serial Data Formats

This section describes each of the Data Format selections available on the RS-232 (Serial Comm) and RS-485 (Remote Port) outputs. Format selection is made as part of the Serial Comm and Remote port configuration. Most applications utilize either Data Format 0 or Data Format 2.

5.1 Format 0

Format 0 includes a time synchronization status character, day of year, time reflecting Time Zone Offset and DST corrections when enabled. Format 0 also includes the DST/Standard Time indicator, and the Time Zone Offset value. Format 0 data structure is shown below:

CR LF I ^ ^ DDD ^ HH:MM:SS ^ DTZ=XX CR LF
where:

CR =	Carriage Return
LF =	Line Feed
I =	Time Sync Status (space, ?, *)
^ =	space separator
DDD =	Day of Year (001 - 366)
HH =	Hours (00-23)
: =	Colon separator
MM =	Minutes (00-59)
SS =	Seconds (00- 60)
D =	Daylight Saving Time indicator (S,I,D,O)
TZ =	Time Zone
XX =	Time Zone offset (00-23)

The leading edge of the first character (CR) marks the on-time point of the data stream.

The time synchronization status character I is defined as described below:

(Space) = Whenever the front panel Time Sync lamp is green.
? = When the receiver is unable to track any satellites and the Time Sync lamp is red.
* = When the receiver time is derived from the battery backed clock or set manual through the Setup Port Interface.

The Daylight Saving Time indicator D is defined as:

S = During periods of Standard time for the selected DST schedule.
I = During the 24-hour period preceding the change into DST
D = During periods of Daylight Saving Time for the selected DST schedule
O = During the 24-hour period preceding the change out of DST

Example: 271 12:45:36 DTZ=08
The example data stream provides the following information:

Sync Status: Time synchronized to GPS

Date: Day 271
Time: 12:45:36 Pacific Daylight Time
D = DST, Time Zone 08 = Pacific Time

5.2 Format 1

This format provides the fully decoded time data stream. Format 1 converts the received day of year data (001-366) to a date consisting of day of week, month, and day of the month. Format 1 also contains a time synchronization status character, year, and time reflecting time zone offset and DST correction when enabled. Format 1 data structure is shown below:

CR LF I ^ WWW ^ DDMMMYY ^ HH:MM:SS CR LF

where:

CR =	Carriage Return
LF =	Line Feed
I =	Time Sync Status (space, ?, *)
^ =	Space separator
WWW =	Day of Week (SUN, MON, TUE, WED, THU, FRI, SAT)
DD =	Numerical Day of Month (^1-31)
MMM =	Month (JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC)
YY =	Year without century (99, 00, 01 etc.)
HH =	Hours (00-23)
: =	Colon separator
MM =	Minutes (00-59)
SS =	Seconds (00 - 60)

The leading edge of the first character (CR) marks the on-time point of the data stream.

The time synchronization status character I is defined as described below:

(Space) = Whenever the front panel time synchronization lamp is green.
? = When the receiver is unable to track any satellites and the time synchronization lamp is red.
* = When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

Example: * FRI 20APR01 12:45:36

The example data stream provides the following information:

Sync Status: The clock is not time synchronized to GPS. Time is derived from the battery backed clock or set manually

Date: Friday, April 20, 2001
Time: 12:45:36

NOTE: Data Format 1 has an available modification that may be made to the data stream structure. Most external systems utilizing Data Format 1 will look for a single digit day of the month for day 1 through day 9, with a space in front of each digit (^1, ^2, ^3 … 10,11…) whereas other systems need to see a two digit day of the month for all days 1 through 9 with a leading 0 instead of a space (01, 02, 03… 10, 11…). If your device requires the two digit day of the month for days 1 through 9, the following procedure will change the Data Format 1 structure to provide this.

Connect to the Serial Setup Interface port with a PC running HyperTerminal OR telnet into the NetClock using the IP address of the unit.

To change Data Format 1 output on a Serial port to a leading 0, type:
ser mod ser[1/2] 1 zero <enter>

(Where 1 or 2 is the desired Serial port number)

To change Data Format 1 output on a Remote RS-485 port to a leading 0, type:
rem mod rem[1/2] 1 zero <enter>

(Where 1 or 2 is the desired Remote port number).

To change Data Format 1 output on a Serial port back to a leading space, type:
Ser mod ser[1/2] none <enter>

(Where 1 or 2 is the desired Remote port number).

To change Data Format 1 output on a Remote RS-485 back to a leading space, type:
rem mod rem[1/2] none <enter>

(Where 1 or 2 is the desired Remote port number).

5.3 Format 2

This format provides a time data stream with millisecond resolution. The Format 2 data stream consists of indicators for time synchronization status, time quality, leap second and Daylight Saving Time. Time data reflects UTC time and is in the 24-hour format. Format 2 data structure is shown below:

NOTE: Format 2 cannot be configured for a Time Zone Offset or with automatic Daylight Saving Time adjustment. Attempting to configure a Local clock using Data Format 2 with either a Time Zone Offset or automatic DST rule will result in an error message.

CR LF IQYY ^ DDD ^ HH:MM:SS.SSS ^ LD

where:

CR	= Carriage Return
LF	= Line Feed
I	= Time Sync Status (space, ?, *)
Q	= Quality Indicator (space, A, B, C, D)
YY	= Year without century (99, 00, 01 etc.)
^	= Space separator
DDD	= Day of Year (001 - 366)
HH	= Hours (00-23 UTC time)
:	= Colon separator
MM	= Minutes (00-59)
SS	= Seconds (00-60)
.	= Decimal Separator
SSS	= Milliseconds (000-999)
L	= Leap Second Indicator (space, L)
D	= Daylight Saving Time Indicator (S,I,D,O)

The leading edge of the first character (CR) marks the on-time point of the data stream.

The time synchronization status character I is defined as described below:

(Space) = Whenever the front panel time synchronization lamp is green.

? = When the receiver is unable to track any satellites and the time synchronization lamp is red.

* = When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The quality indicator Q provides an inaccuracy estimate of the output data stream. When the receiver is unable to track any GPS satellites, a timer is started. Table 6-2: Table of Quality Indicators lists the quality indicators and the corresponding error estimates based upon the GPS receiver 1 PPS stability, and the time elapsed tracking no satellites. The Tracking Zero Satellites timer and the quality indicator reset when the receiver reacquires a satellite.

Quality	Time (hours)	TCXO Error (Standard configuration) (milliseconds)	OCXO Error (Option 05) (milliseconds)	Rubidium Error (Option 04) (microseconds)
Space	Lock	<1	<0.01	<0.3
A	<10	<10	<0.72	<1.8
B	<100	<100	<7.2	<18
C	<500	<500	<36	<90
D	>500	>500	>36	>90

Table 5-1: Table of Quality Indicators

The leap second indicator L is defined as:

(Space) = When a leap second correction is not scheduled for the end of the month.
L = When a leap second correction is scheduled for the end of the month.

The Daylight Saving Time indicator D is defined as:

S = During periods of Standard time for the selected DST schedule.
I = During the 24-hour period preceding the change into DST.
D = During periods of Daylight Saving Time for the selected DST schedule.
O = During the 24-hour period preceding the change out of DST.

Example: ?A01 271 12:45:36.123 S

The example data stream provides the following information:

Sync Status: The clock has lost GPS time sync. The inaccuracy code of “A” indicates the expected time error is <10 milliseconds.

Date: Day 271 of year 2001.

Time: 12:45:36 UTC time, Standard time is in effect.

5.4 Format 3

Format 3 provides a format identifier, time synchronization status character, year, month, day, time with time zone and DST corrections, time difference from UTC, Standard time/DST indicator, leap second indicator and on-time marker. Format 3 data structure is shown below:

FFFFI^YYYYMMDD^HHMMSS±HHMMD L # CR LF

where:

FFFF	= Format Identifier (0003)
I	= Time Sync Status (Space, ? *)
^	= Space separator
YYYY	= Year (1999, 2000, 2001 etc.)
MM	= Month Number (01-12)
DD	= Day of the Month (01-31)
HH	= Hours (00-23)
MM	= Minutes (00-59)
SS	= Seconds (00-60)
±	= Positive or Negative UTC offset (+,-) Time Difference from UTC
HHMM	= UTC Time Difference Hours, Minutes (00:00-23:00)
D	= Daylight Saving Time Indicator (S,I,D,O)
L	= Leap Second Indicator (space, L)
#	= On time point
CR	= Carriage Return
LF	= Line Feed

The time synchronization status character I is defined as:

(Space) =	Whenever the front panel time synchronization lamp is green.
? =	When the receiver is unable to track any satellites and the time synchronization lamp is red.
* =	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The time difference from UTC, ±HHMM, is selected when the Serial Comm or Remote port is configured. A time difference of -0500 represents Eastern Time. UTC is represented by +0000.

The Daylight Saving Time indicator D is defined as:

S =	During periods of standard time for the selected DST schedule.
I =	During the 24-hour period preceding the change into DST.
D =	During periods of Daylight Saving Time for the selected DST schedule.
O =	During the 24-hour period preceding the change out of DST.

The leap second indicator L is defined as:

(Space) =	When a leap second correction is not scheduled at the end of the month.
L =	When a leap second correction is scheduled at the months end.

Example: 0003 20010415 124536-0500D #

The example data stream provides the following information:

Data Format: 3

Sync Status: Time Synchronized to GPS.

Date: April 15, 2001.

Time: 12:45:36 EDT (Eastern Daylight Time). The time difference is 5 hours behind UTC.

Leap Second: No leap second is scheduled for this month.

5.5 Format 4

Format 4 provides a format indicator, time synchronization status character, modified Julian date, time reflecting UTC with 0.1 millisecond resolution and a leap second indicator. Format 4 data structure is shown below:

FFFFIMJDXX^HHMMSS.SSSS^L CR LF

where:

FFFF	= Format Identifier (0004)
I	= Time Sync Status (Space, ? *)
MJDXX	= Modified Julian Date
HH	= Hours (00-23 UTC time)
MM	= Minutes (00-59)
SS.SSSS	= Seconds (00.0000-60.0000)
L	= Leap Second Indicator (^, L)
CR	= Carriage Return
LF	= Line Feed

The start bit of the first character marks the on-time point of the data stream.

The time synchronization status character I is defined as:

(Space) =	Whenever the front panel time synchronization lamp is green.
? =	When the receiver is unable to track any satellites and the time synchronization lamp is red.
* =	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The leap second indicator L is defined as:

(Space) =	When a leap second correction is not scheduled at the end of the month.
L =	when a leap second correction is scheduled at the months end.

Example: 0004 50085 124536.1942 L

The example data stream provides the following information:

Data format:	4
Sync Status:	Time synchronized to GPS.
Modified Julian Date:	50085
Time:	12:45:36.1942 UTC
Leap Second:	A leap second is scheduled at the end of the month.

5.6 Format 7

This format provides a time data stream with millisecond resolution. The Format 7 data stream consists of indicators for time synchronization status, leap second and Daylight Saving Time. Time data reflects UTC time and is in the 24-hour format. Format 7 data structure is shown below:

NOTE: Format 7 cannot be configured for a Time Zone Offset or with automatic Daylight Saving Time adjustment. Attempting to configure a Local clock using Data Format 7 with either a Time Zone Offset or automatic DST rule will result in an error message.

CR LF I^YY^DDD^HH:MM:SS.SSSL^D CR LF

where:

CR	= Carriage Return
LF	= Line Feed
I	= Time Sync Status (space, ?, *)
YY	= Year without century (99, 00, 01 etc.)
^	= Space separator
DDD	= Day of Year (001 - 366)
HH	= Hours (00-23 UTC time)
:	= Colon separator
MM	= Minutes (00-59)
SS	= Seconds (00-60)
.	= Decimal Separator
SSS	= Milliseconds (000-999)
L	= Leap Second Indicator (space, L)
D	= Daylight Saving Time Indicator (S,I,D,O)

The leading edge of the first character (CR) marks the on-time point of the data stream.

The time synchronization status character I is defined as described below:

(Space) =	Whenever the front panel time synchronization lamp is green.
? =	When the receiver is unable to track any satellites and the time synchronization lamp is red.
* =	When the receiver time is derived from the battery backed clock or set manually through the Setup Port Interface.

The leap second indicator L is defined as:

(Space) = When a leap second correction is not scheduled for the end of the month.
L = When a leap second correction is scheduled for the end of the month.

The Daylight Saving Time indicator D is defined as:

S = During periods of Standard time for the selected DST schedule.
I = During the 24-hour period preceding the change into DST.
D = During periods of Daylight Saving Time for the selected DST schedule.
O = During the 24-hour period preceding the change out of DST.

Example: ? 01 271 12:45:36.123 S

The example data stream provides the following information:

Sync Status: The clock has lost GPS time sync.
Date: Day 271 of year 2001.
Time: 12:45:36 UTC time, Standard time is in effect.

5.7 Format 8

Format 8 includes a time synchronization status character, the four digit year, day of year, time reflecting Time Zone Offset and DST corrections when enabled. Format 8 also includes the DST/Standard Time indicator, and the Time Zone Offset value. Format 8 data structure is shown below:

CR LF I ^ ^YYYY^ DDD ^ HH:MM:SS ^ D+XX CR LF or
CR LF I ^ ^YYYY^ DDD ^ HH:MM:SS ^ D-XX CR LF

where

CR	= Carriage Return
LF	= Line Feed
I	= Time Sync Status (space, ?, *)
YYYY	= Four digit year indication
^	= Space separator
DDD	= Day of Year (001 - 366)
HH	= Hours (00-23)
:	= Colon separator
MM	= Minutes (00-59)
SS	= Seconds (00 - 60)
D	= Daylight Saving Time indicator (S,I,D,0)
XX	= Time Zone Switch Setting (+/- 00 to 12)

The leading edge of the first character (CR) marks the on-time point of the data stream.

Time sync status character I is described below:

= (space) when the NetClock is synchronized to UTC source.
= * when the NetClock time is set manually.
= ? when the NetClock has not achieved or has lost synchronization to UTC source.

The time and date can be set to either local time or UTC time, depending upon the configuration of the output port.

5.8 Format 90

Format 90 provides a position data stream in NMEA 0183 GPGGA GPS Fix data format. The Format 90 data structure is shown below:

$GPGGA,HHMMSS.SS,ddmm.mmmm,n,dddmm.mmmm,e,Q,SS,YY.y,+AAAAA.a,M,,,,*CC CR LF

where:

$GP =	GPS System Talker
GGA =	GPS Fix Data Message
HHMMSS.SS =	Latest time of Position Fix, UTC. This field is blank until a 3D fix is acquired
ddmm.mmmm,n =	Latitude
dd =	degress, 00...90
mm.mmmm =	minutes, 00.0000....59.9999
n =	direction, N = North, S = South
dddmm.mmmm,e =	Longitude
ddd =	degress, 000...180
mm.mmmm =	minutes, 00.0000....59.9999
e =	direction, E = East, W = West
Q =	Quality Indicator,
0 =	No 3D fix
1 =	3D fix
SS =	Number of satellites tracked, 0...8
YY.Y =	Dilution of precision, 00.0...99.9
+AAAAA.a,M =	Antenna height in meters, referenced to mean sea level
,,,, =	Fields for geoidal separation and differential GPS not supported
cc =	Check sum message, HEX 00...7F Check sum calculated by Xoring all bytes between $ and *.
CR =	Carriage Return
LF =	Line Feed

Example:
$GPGAA,151119.00,4307.0241,N,07729.2249,W,1,06,03.2,+00125.5,M,,,*3F

The example data stream provides the following information:

Time of Position Fix:	15:11:19.00 UTC
Latitude:	43° 07.0241’ North
Longitude:	77° 29.2249’ West
Quality:	3D fix
Satellites Used:	6
Dilution of Precision:	3.2
Antenna Height:	+125.5 meters above sea level
Check Sum:	3

6 Serial Setup Interface Commands

The NetClock can be configured using the serial setup interface port and a terminal emulation program as discussed in Section 3.2. At the Command Line Interface (CLI), the user can manage files and configure product settings.

The available CLI commands are as follows:

```
time        - time
reboot      - reboot [app]
halt        - halt
log         - log COMMAND OBJECT [ HANDLE ]
option      - option COMMAND [OPTION | PRODUCT] [VALUE]
ltc         - ltc COMMAND [INDEX | NAME] [...]
net         - net COMMAND [Arguments]
sys         - sys COMMAND [Arguments]
mdo         - mdo COMMAND [Arguments]
ser         - ser COMMAND SERIAL [Arguments]
rem         - rem COMMAND REMOTE [Arguments]
irig        - irig COMMAND ARG
frq         - frq COMMAND INDEX [Arguments]
stc         - stc COMMAND [Arguments]
```

One additional command, **help**, displays the available commands at the CLI. Typing **help** and a specific command (for example, **help time**, or **help option**) and then pressing the enter key displays detailed information about the command.

NOTE: Commands typed at the CLI are case-sensitive. All terms and commands entered must be lower-case.

6.1 time

```
help time
Use the 'time' command to read the current system date and time.
USAGE: time
```

6.2 reboot

The ***reboot*** is used to warm-boot the unit without having to disconnect or reconnect the power supply. The ***reboot*** command is intended only for administrators, and is available at the *admin* security level.

NOTE: This command provides a convenient way to remotely update application software in that the unit will automatically execute the most recent image in /sys/bin/.

```
help reboot
This command is used to immediately reboot a unit.
The 'app' option is used to restart the application. Normally the unit
reboots to the application, unless the optional parameter is specified
to 'bootloader' which it will reboot to the bootloader.
USAGE: reboot [app]
    app  - Reboot to application.
```

NOTE: Do not reboot the unit while file uploads are in progress. Do not reboot the unit with non-application images are located in /sys/bin/. If either of these conditions is not fulfilled, the unit may fail to boot the application image, which could result in a unit that function incorrectly or not at all.

6.3 log

```
help log
Use the 'log' command to access and manage the log system.
USAGE: log COMMAND OBJECT [ HANDLE ]
  COMMAND
    show   - Shows the contents of a log.
    get    - Gets the record #[HANDLE] from a log.
  OBJECT
    j      - Journal log
    a      - Alarm log
    g      - GPS qualification Log
    o      - Operational log
    x      - Oscillator log
    d      - Dialout log
    n      - NTP log
    r      - Event relay log
    t      - Authorization log
    u      - Update log
  HANDLE : Record number to access. The first record is 0.
```

6.4 option

```
help option
The 'option' commands provide a means to set, clear and display
product configuration options.
USAGE: option COMMAND [OPTION | PRODUCT] [VALUE]
  COMMAND
    display - Displays current option settings.
    enable  - Enables options after verifying the hash value.
```

6.5 ltc

The ltc command is used to create up to five Local clocks. Local clocks allow many of the output ports to be able to provide time data as local time instead of just UTC time. This command requires admin level login.

```
help ltc
The 'ltc' group of commands are used to manage the local time clocks.
USAGE: ltc COMMAND [INDEX | NAME] [...]
  COMMAND = {disp | create | delete | tz | dst}
    disp   - Displays information about the local clock.
    Create - Creates a new local clock. Multiple consecutive
             spaces in the name will be reduced to a single space
    delete - Deletes a local clock at the specified index.
    tz     - Assigns a new time zone offset for the local clock.
```

```
    dst   - Assigns a new daylight saving rule to the clock.
```

6.6 net

The command, ***net***, is used to configure the network interface. The ***net*** command consists of a set of subcommands that are used to get, set or change each individual network setting. Some of the network settings require admin level security in order to set or change them.

```
help net
The 'net' group of commands are used to manage network interface
USAGE: net COMMAND [Arguments]
  COMMAND
    Config      - Configure IP settings.
    show        - Displays network configurations.
    Daytime     - Enable/disable Daytime.
    time        - Enable/disable UNIX time.
    telnet      - Enable/disable Telnet.
    ftp         - Enable/disable FTP
    http        - Enable/disable HTTP.
    https       - Enable/disable secure HTTP.
    ssh         - Enable/disable SSH.
```

6.7 sys

```
help sys
The sys group of commands are used to retrieve information about the
system.
USAGE: sys COMMAND [Arguments]
  COMMAND
    mem  - Display memory information. Use v for verbose mode.
```

6.8 mdo

The mdo command is used to configure the dial-out modem option if it is installed. The mdo command consists of a set of subcommands used to control logs and modem configuration.

```
help mdo
The mdo group of commands are used to setup the modem.
USAGE: mdo COMMAND [Arguments]
  COMMAND
    mode     - Sets the Serial Setup Interface into a 'console' or
               'modem' mode.
    Baud rate can be specified in modem mode.
    dialnow  - Dials out immediately.
    baud     - Sets baud rate specified by user.
ITU-R protocols use 1200 and ACTS protocols use 9600. NIST ACTS may
support either, however 9600 is recommended.
    speaker  - Sets modem speaker on/off.
```

6.9 ser

The ser command allows the rear panel Serial ports to be configured from the console. They require admin level login.

```
help ser
The ser group of commands are used to setup serial ports RS-232.
USAGE: ser COMMAND SERIAL [Arguments]
  COMMAND
    disp   - Displays the current serial port settings.
    all    - Configures all settings of a serial port.
    fmt    - Configures the format of the serial port output.
    req    - Sets the request character on a serial port.
    ltc    - Sets the reference clock on the serial output.
           To add/configure local clocks, use command 'ltc'
    baud   - Configures the baud rate of a serial port.
```

6.10 rem

The rem command allows the rear panel Remote output(s) to be configured from the console port. This command requires admin level login to modify.

```
help rem
The rem group of commands are used to setup remote serial ports RS485.
USAGE: rem COMMAND REMOTE [Arguments]
  COMMAND
    disp   - Displays the current remote serial port settings.
    all    - Configures all settings of a remote serial port.
    fmt    - Configures the format of the serial port output
    ltc    - Sets the reference clock on the remote serial
           output.
    To add/configure local clocks, use command 'ltc'
    baud   - Configures the baud rate of a remote serial port.
```

6.11 irig

```
help irig
The 'irig' group of commands are used to control the irig subsystem.
USAGE: irig COMMAND ARG
  COMMAND = {disp | b | brb | e | amp | ltc | sig}
    disp   - Display the current IRIG port settings.
    b      - Sets the irig output to format B.
    brb    - Sets the irig output to format B Rubidium.(TTL
           level)
           This option is only available on Rubidium units.
    e      - Sets the irig output to format E.
    amp    - Sets the amplitude level for AM signals.
    ltc    - Sets the reference clock for the IRIG output.
    sig    - Sets the signature control of the IRIG port.
```

6.12 frq

```
help frq
The frq group of commands are used manage frequency interfaces.
USAGE: frq COMMAND INDEX [Arguments]
  COMMAND
    mode         - Sets the signature control mode.
    status       - Displays the status of the selected frequency
                   output.
```

6.13 stc

```
help stc
The stc group of commands are used to setup serial time code input.
USAGE: stc COMMAND [Arguments]
 COMMAND
disp     - Displays the current serial time code input settings.
 all     - Configures all settings of serial time code input.
 fmt     - Configures the format of the serial time code input.
baud     - Configures the baud rate of serial time code input.
year     - Configures the year used by format 0 serial time code input
```

7 Options

Spectracom offers several options for the 9300 Series.

Option	Description	9383	9389	9388
02	Front panel display & Second Serial Port/Remote Port	STANDARD	OPTIONAL	NO
03	Dial-Out Modem & ACTS Server	OPTIONAL	OPTIONAL	NO
04	Rb (Rubidium) Oscillator *	OPTIONAL	OPTIONAL	NO
05	OCXO Oscillator *	OPTIONAL	OPTIONAL	NO
06	IRIG Input	OPTIONAL	OPTIONAL	NO
07	SAASM GPS Receiver	OPTIONAL	OPTIONAL	NO
08	SPS GPS Receiver	STANDARD	STANDARD	NO
09	TCXO Oscillator *	STANDARD	STANDARD	STANDARD

*Choose one oscillator only.

Please contact Spectracom's Sales department for information regarding any options you do not yet have that you may wish to purchase. Those options requiring additional explanation are detailed herein.

7.1 Option 03: Modem

7.1.1 Option 03 Basics

Option 03 provides the NetClock with the capability to use a modem to dial-out via an analog phone line for time retrieval if GPS reception is either lost or cannot be obtained due to site limitations. The modem can be configured in the software as either the primary external time reference or it can also be configured as a Secondary/Backup reference in case the primary reference is lost.

The modem interfaces to the NetClock via the Serial Setup Interface located on the rear of the NetClock. This dual-function port provides the capability to initially configure the network settings and is also the interface for the modem.

If not initially purchased with the unit, Option 03 can be enabled (turned on) in the field. Please contact our Sales department to purchase this option. You will be sent a Hash key that can be entered in the NetClock to enable the security algorithms. The purchase of the option includes a Spectracom supplied compatible modem.

NOTE: The modem **MUST** be **Hayes AT** compatible and configured for this mode of operation to operate correctly with the unit. The Spectracom supplied modem is Hayes AT compatible.

NOTE: If the NetClock's admin or user passwords are changed, the NetClock must be rebooted after this change to ensure proper modem operation.

7.1.2 Modem Installation

The provided DB9 to DB9 null modem cable connects to the rear of the modem using a DB9 to DB25 adapter (also provided).

NOTE: The switches on the rear of the modem (Figure 7-1, inset) must be set for proper operation. Set Switches 3 and 8 down. All other switches should be up.

1. Connect one DB9 side of the null modem cable to the to the Serial Setup port located on the rear of the NetClock. Connect the other end of the cable to the provided adapter and connect the adapter to the modem.

2. Connect the CAT2 telephone cable from the analog phone line to the modem.

3. Connect the modem power adapter to a power outlet.

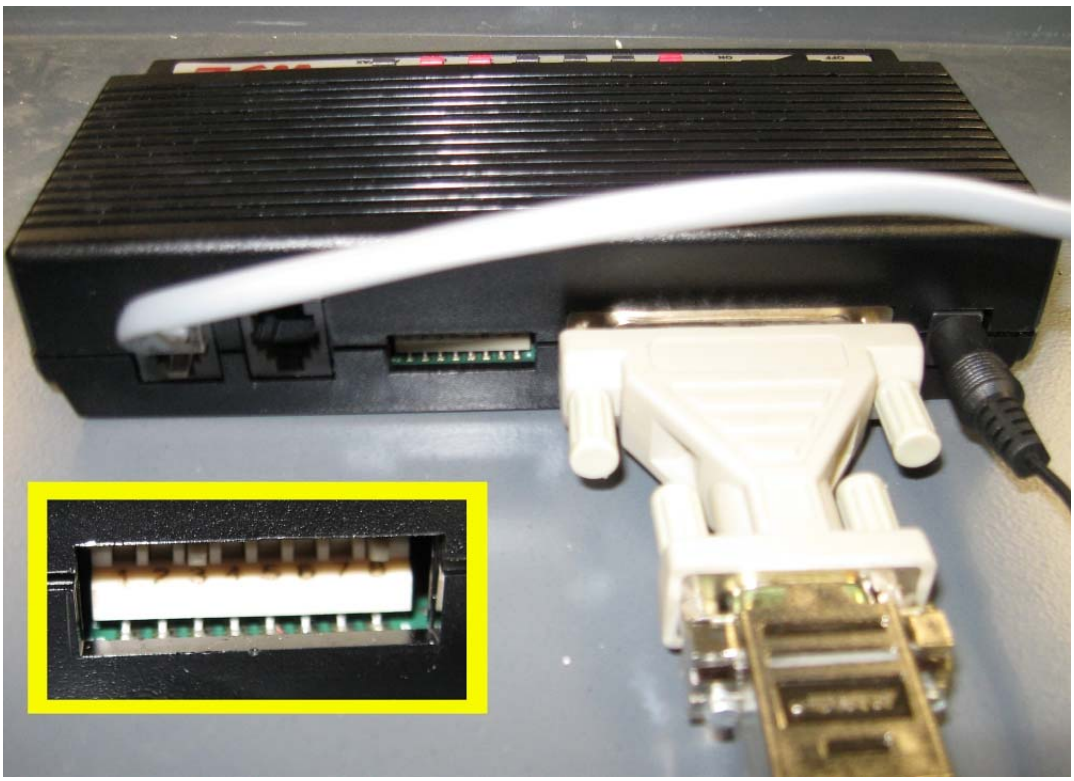


Figure 7-1: Modem Switches

7.1.3 Modem Configuration

The modem is configured from the System Modem Configuration screen, which includes the Port mode pull-down menu. The modem is connected to the Serial Setup port for normal operation. The pull-down menu allows the operator to select the mode in which the serial setup port will operate. Two options are available: Console mode and Client mode. The screen and the menu available at the left of the screen vary depending on the mode.

Console Mode: In this mode (Figure 7-2), Serial Setup port can be connected with a serial cable to a computer with a serial terminal program running. The serial setup software commands can then be used to interface with the unit. The modem operation will not be available while selected to this mode.

Client Mode: In this mode (Figure 7-3), the Serial Setup port can be connected to a modem for dialing out. The Serial Setup port will be unavailable for network configuration while in this mode.

NOTE: If the NetClock is switched repeatedly between Console and Client modes, the modem application may stop functioning. Reboot the NetClock to clear this condition.

ACTS Server Mode: This mode (Figure 7-4) configures the NetClock to answer telephone calls, using the modem, when connected to an analog telephone line. The modem connects to the NetClock in the same manner as for Client mode.

NOTE: Click "Submit" to apply the change to the modem mode. Return to Modem Configuration to access the screen options for Client mode.

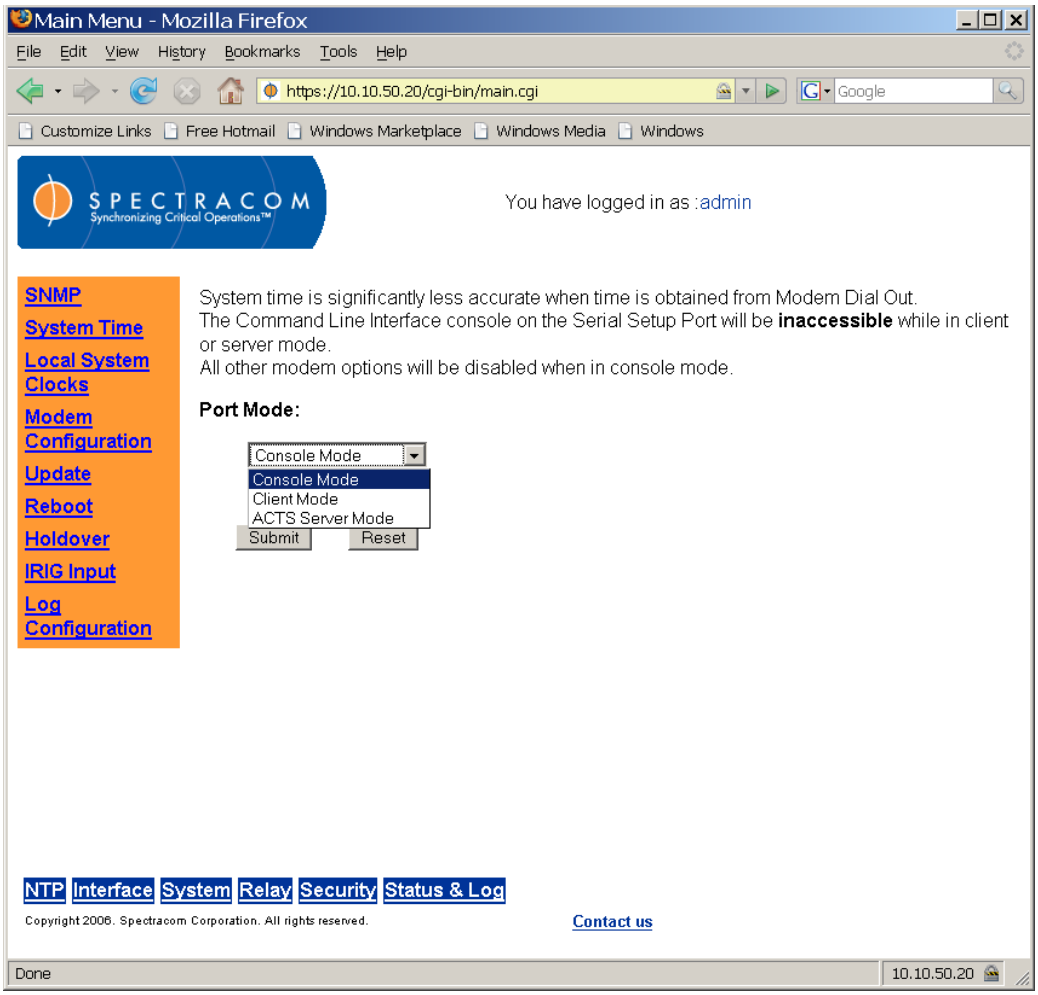


Figure 7-2: System Modem Configuration Screen, Console Mode

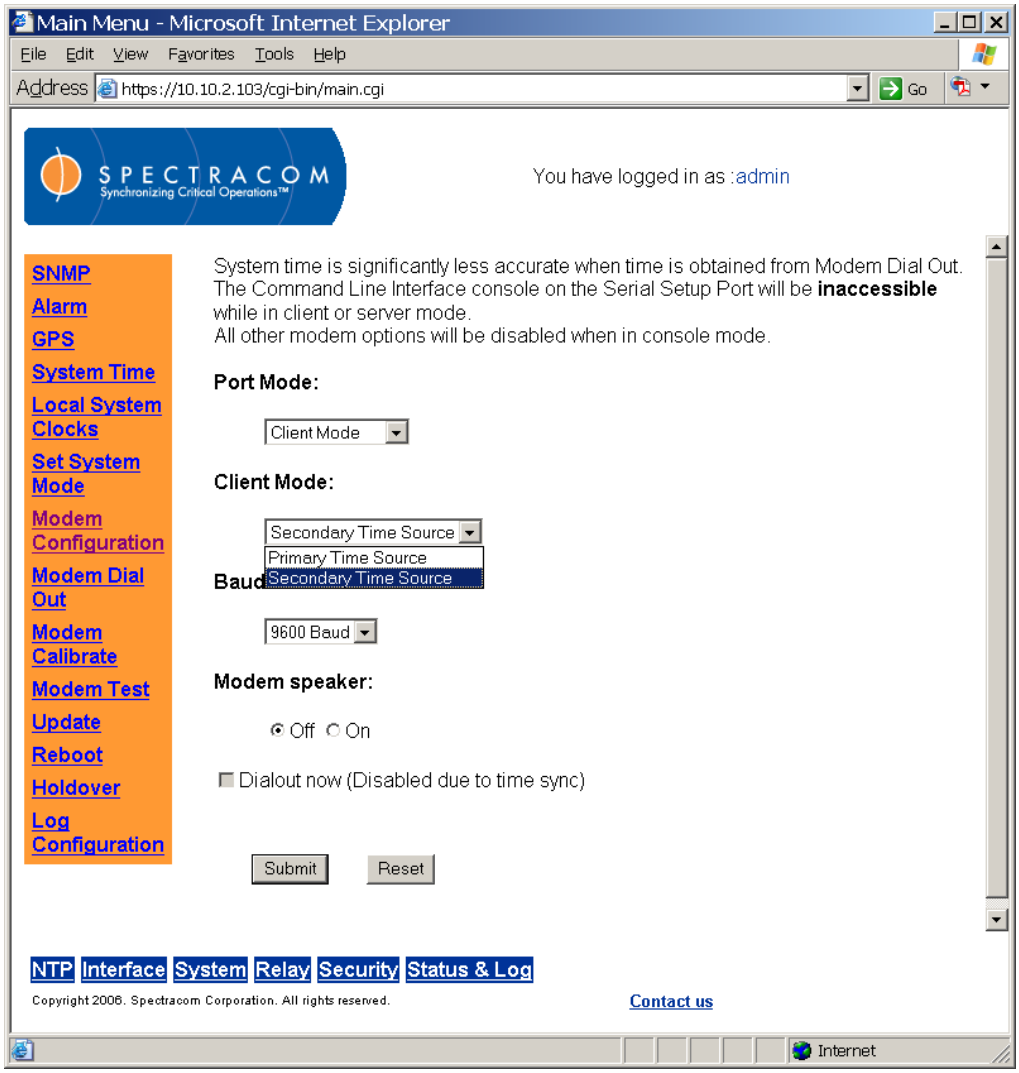


Figure 7-3: System Modem Configuration Screen, Client Mode

After selecting Client mode, submitting the change, and returning to the Modem Configuration screen, the user may configure the modem through the Web UI:

Primary/Secondary Time Source: The modem can be configured as either the primary reference or a secondary/back-up reference. In the Secondary/Back-up mode of operation, all GPS antenna problem alarms (indicating a short or open in the antenna cable) and SNMP traps associated with the GPS reference input will be fully enabled. By contrast, when Primary Time Source is selected, the antenna problem alarm and associated SNMP traps for the antenna will not be generated. No indication of a problem with the GPS cable will be present or available. The Client mode of operation does not affect the ability to receive GPS.

NOTE: If a unit initially operates without a GPS reference and primary mode of operation is selected, and a GPS antenna is later connected, the mode of operation should be changed to Secondary Time Source. This enables the GPS antenna problem alarms, which can be used in troubleshooting the system.

Baud rate: Baud rates of 1200 and 9600 are available and can be selected from the pull-down menu.

Modem speaker: Toggles the modem speaker on or off during dial out.

Dialout now: (Only available in Client mode and only when the unit is not in time sync). Checking this box and clicking submit will prompt the dial out modem software to attempt an immediate dial out procedure with the current settings if the unit is currently out of sync. When a unit is configured in client mode while it is in time sync, the "Dialout now" checkbox will be greyed-out (disabled).

7.1.4 ACTS Server Mode

The ACTS Server feature has been designed to operate similarly to the Automated Computer Time Service (ACTS) provided by the National Institute of Standards and Technology (NIST). It is compatible with client programs that dial out to the NIST ACTS service for time synchronization, such as the NetClock when configured in Client mode. For best accuracy, Spectracom recommends using a NetClock in Client mode in conjunction with a NetClock operating in ACTS Server mode.

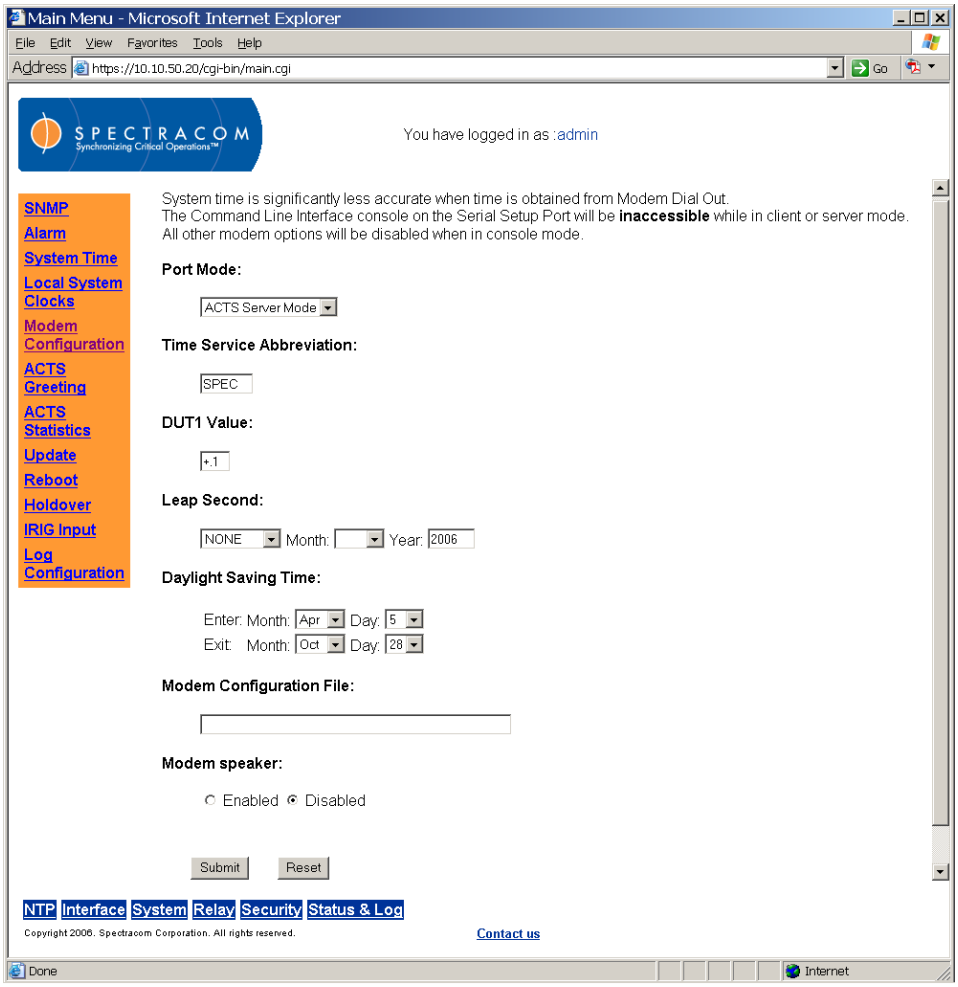


Figure 7-4: ACTS Server Mode Selected

Time Service Abbreviation: This field indicates the source from which a dial-out client is receiving Universal Coordinated Time (UTC). It is inserted in the ACTS timing message sent to the modem client. A time service abbreviation of SPEC will appear in the timing message as UTC (SPEC).

DUT1 Value: This is a correction factor for converting UTC to an older form of Universal Time. The value should always be a number between -.8 and .8 seconds. Adding DUT1 to UTC produces UT1 (a specific measure of time related to the rotation of Earth). The three-digit string entered in this field appears in the time messages sent to the modem client.

Leap Second: This field allows the user to specify the addition or removal of a leap second as well as the month and year in which this addition or removal will occur. The ACTS Server uses this information to notify the modem client of a pending leap second. It does so through time messages sent to the modem client.

Daylight Saving Time: This field is used to specify the month and day of the current year in which Daylight Saving Time (DST) is entered and exited. This information is included in the time messages sent to the modem client.

Modem Configuration File: The ACTS Server uses built-in, Hayes-compatible commands to configure the modem. Some modems may support additional or different commands, which may be required for proper configuration. If a *modem configuration file* is specified, the ACTS Server will use the commands in that specified file to configure the modem, rather than using its built-in Hayes-compatible commands.

Modem Speaker: Clicking the appropriate radio button toggles the modem speaker on or off during dial out.

The ACTS Server Greeting (Figure 7-5), accessible using the left-hand menu, is a message sent to a modem client when a connection is made. The Acts Server Greeting screen allows the user to customize the greeting message for the specific application.

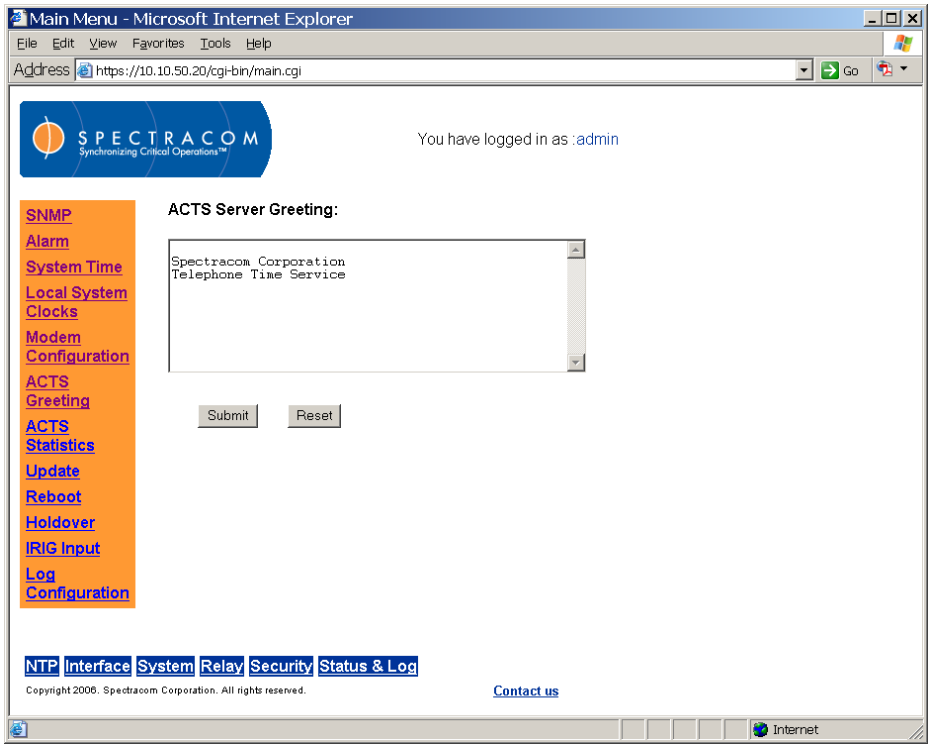


Figure 7-5: ACTS Server Greeting

The ACTS Server Statistics screen (Figure 7-6), accessible using the left-hand menu, provides all data for the current day and the previous day. For each day, it shows the number of attempted and completed calls during each hour of that day. This data is helpful in analyzing modem usage and balancing modem client call times.

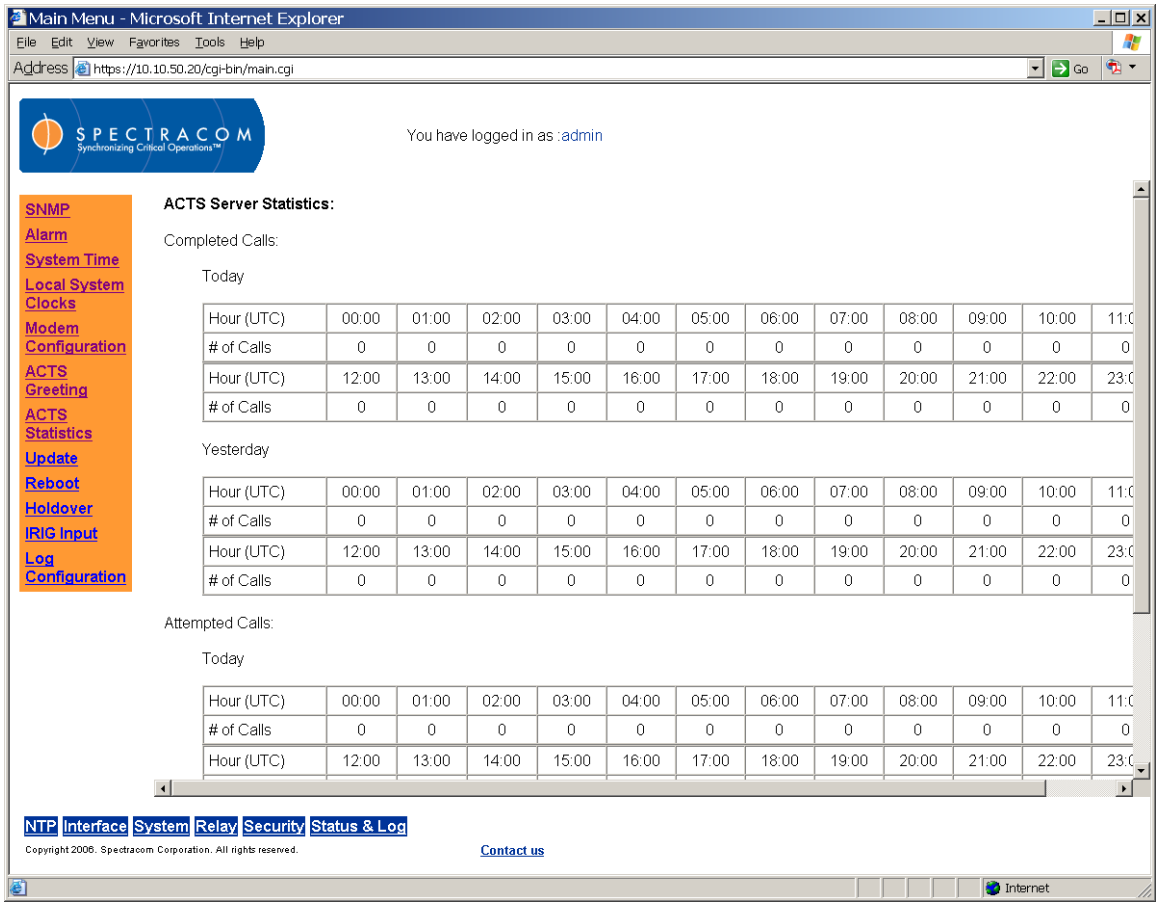

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://10.10.50.20/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
SNMP
Alarm
System Time
Local System Clocks
Modem Configuration
ACTS Greeting
ACTS Statistics
Update
Reboot
Holdover
IRIG Input
Log Configuration
ACTS Server Statistics:
Completed Calls:
Today
Hour (UTC) 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:0
# of Calls 0 0 0 0 0 0 0 0 0 0 0 0
Hour (UTC) 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:0
# of Calls 0 0 0 0 0 0 0 0 0 0 0 0
Yesterday
Hour (UTC) 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:0
# of Calls 0 0 0 0 0 0 0 0 0 0 0 0
Hour (UTC) 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:0
# of Calls 0 0 0 0 0 0 0 0 0 0 0 0
Attempted Calls:
Today
Hour (UTC) 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:0
# of Calls 0 0 0 0 0 0 0 0 0 0 0 0
Hour (UTC) 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:0
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Internet

Figure 7-6: ACTS Server Statistics

The ACTS Server Log (Figure 7-7) helps the user monitor the behavior of the ACTS server daemon, including when it is started, when it is stopped, and how it is configured. The log records information about each time message it sends to the modem client. Data contained in the log is helpful in troubleshooting when there is a problem in communication between the ACTS server and modem client.

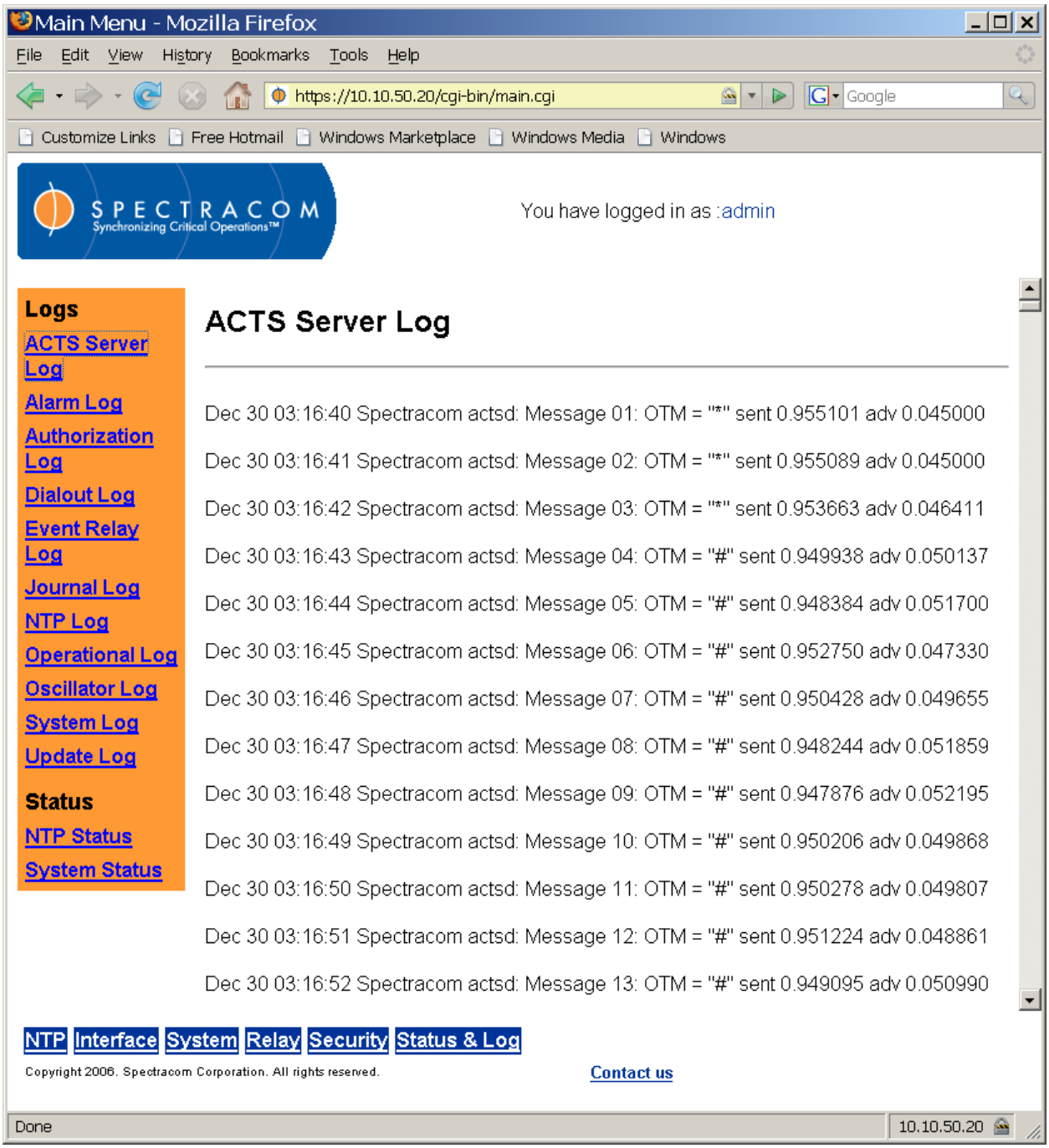

Main Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.10.50.20/cgi-bin/main.cgi
Google
Customize Links Free Hotmail Windows Marketplace Windows Media Windows
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
ACTS Server Log
Alarm Log
Authorization Log
Dialout Log
Event Relay Log
Journal Log
NTP Log
Operational Log
Oscillator Log
System Log
Update Log
Status
NTP Status
System Status
ACTS Server Log
Dec 30 03:16:40 Spectracom actsd: Message 01: OTM = "*" sent 0.955101 adv 0.045000
Dec 30 03:16:41 Spectracom actsd: Message 02: OTM = "*" sent 0.955089 adv 0.045000
Dec 30 03:16:42 Spectracom actsd: Message 03: OTM = "*" sent 0.953663 adv 0.046411
Dec 30 03:16:43 Spectracom actsd: Message 04: OTM = "#" sent 0.949938 adv 0.050137
Dec 30 03:16:44 Spectracom actsd: Message 05: OTM = "#" sent 0.948384 adv 0.051700
Dec 30 03:16:45 Spectracom actsd: Message 06: OTM = "#" sent 0.952750 adv 0.047330
Dec 30 03:16:46 Spectracom actsd: Message 07: OTM = "#" sent 0.950428 adv 0.049655
Dec 30 03:16:47 Spectracom actsd: Message 08: OTM = "#" sent 0.948244 adv 0.051859
Dec 30 03:16:48 Spectracom actsd: Message 09: OTM = "#" sent 0.947876 adv 0.052195
Dec 30 03:16:49 Spectracom actsd: Message 10: OTM = "#" sent 0.950206 adv 0.049868
Dec 30 03:16:50 Spectracom actsd: Message 11: OTM = "#" sent 0.950278 adv 0.049807
Dec 30 03:16:51 Spectracom actsd: Message 12: OTM = "#" sent 0.951224 adv 0.048861
Dec 30 03:16:52 Spectracom actsd: Message 13: OTM = "#" sent 0.949095 adv 0.050990
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Done
10.10.50.20

Figure 7-7: ACTS Server Log

7.1.5 Modem Dial-Out Setup

The modem dial-out feature is used as either a Secondary/Backup time reference when all other external time references become unavailable or can also be used as a primary reference if an external reference is not available for use (Such as the inability to receive GPS at a particular

location). The System Modem Configuration screen (Figure 7-2) provides options to configure the operation of the dial-out modem feature from the left-hand menu. All fields will display the current system settings.

7.1.6 Modem Dialout

The Modem Dialout screen (Figure 7-8) is used to annotate the phone number used to obtain the time from and to determine how often the modem will be used to retrieve the current time.

Phone Numbers:
Prefix: The phone prefix is a number(s) that need to be dialed to reach an outside line.

Predefined: Stores two predefined number NIST-Colorado and NIST-Hawaii. These are the phone numbers to the National Institute of Standards and Technology modem time service.

Specified Number: This field will take any phone number that the user would like to use to dial out to obtain time.

Try Calling: This field specifies how many times the dial out modem software will try to connect to the selected phone number. Setting this field's value to 0 will generate a warning because it will prevent any dial out to be made in any condition, effectively disabling the modem dial out feature.

Call Interval:
The call interval is used to manually configure how often the modem should dial-out for Time verification calls when the unit is in the holdover mode and time synchronization is normally derived from GPS (Secondary/Backup mode of operation) or time synchronization calls when the modem is selected as the primary mode of operation.

To prevent a leap second occurrence from being missed and a one second error being inserted into the NetClock, we recommend the Time Verification calls be placed less than once-per-month. Setting the Time Verification call period to longer than once-per-month can result in a one second error from the time a leap second is asserted by NIST until the next time verification/time synchronization call is placed.

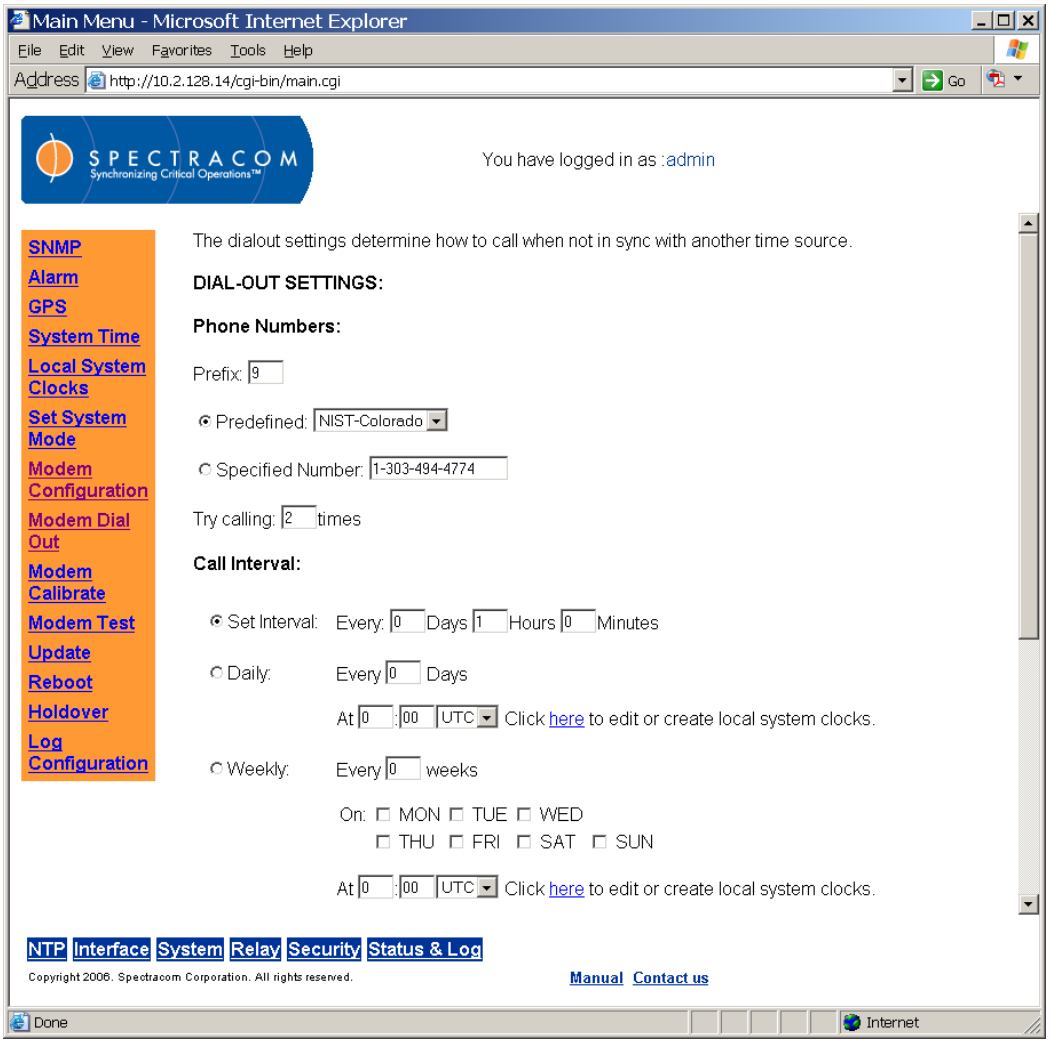


Figure 7-8: System Modem Dial Out Screen (1 of 2)

To help prevent a loss of time synchronization condition from occurring, the call interval should be configured for a value of less than the holdover period. This will prevent the holdover period from expiring (which will cause loss of Time Sync) because the modem was configured to dial-out after the holdover expired. For example, if the holdover period is set for two weeks, the call interval should be set to dial-out less than every two weeks. Otherwise, holdover will expire before the modem is scheduled for a dial-out and time synchronization will be lost.

Boot:
This field specifies how long the modem software will wait after being powered up to check the unit's time synchronization status. If this time expires and the unit has not achieved time synchronization yet, the modem software will automatically dial out with the current settings at that time. Note that changes to this timer's settings will not change the timeout of the current countdown if it has already begun (e.g. If the timer is set to 1 hour and then rebooted, the unit will countdown to 1 hour at power up. Changing the timer's settings to 30 minutes will not affect the current countdown. The new 30 minutes value will only be used if another power cycle occurred). To skip the initial countdown, use the Dialout Now feature on the Modem Configuration screen.

.

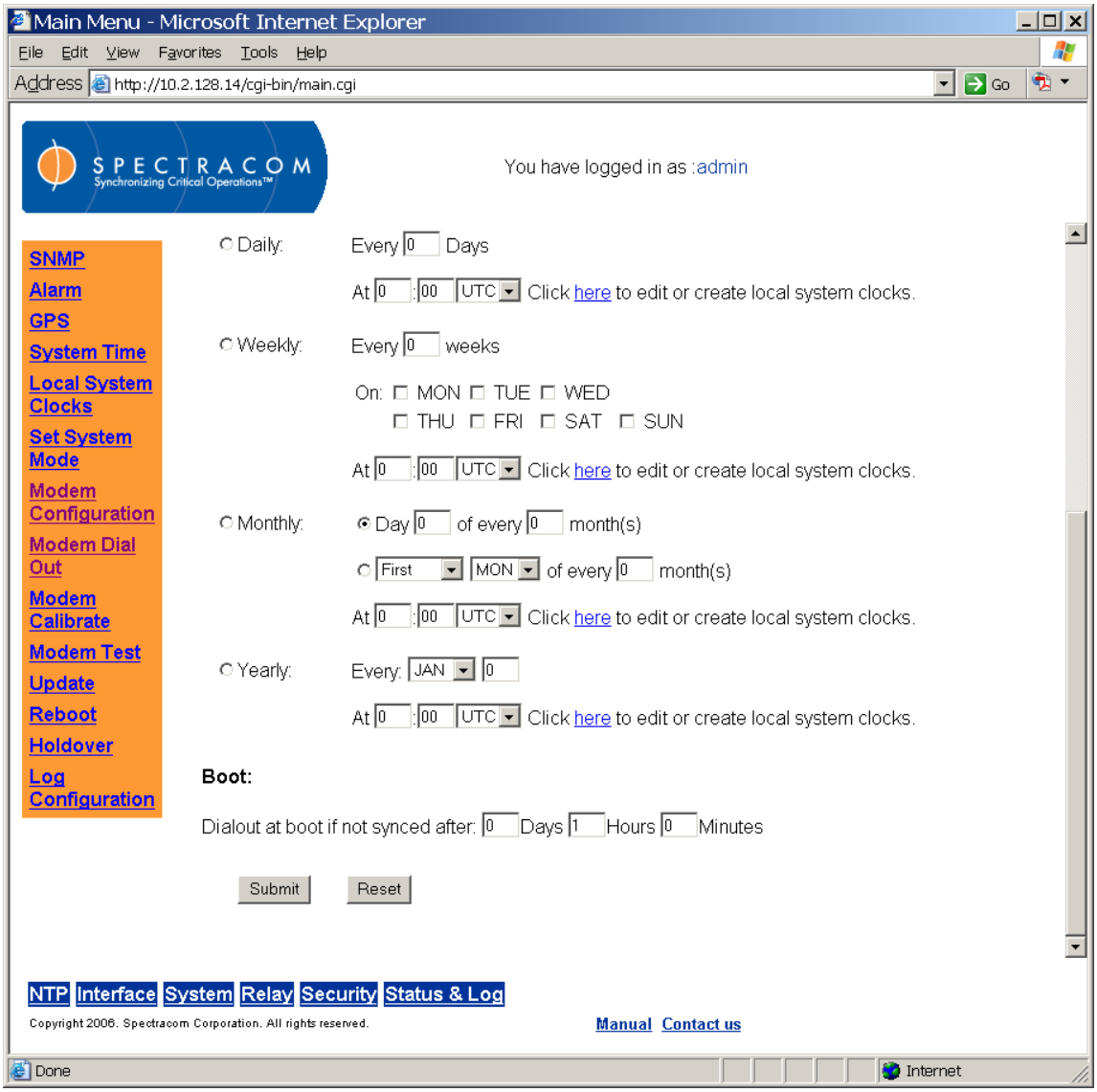

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.2.128.14/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
SNMP
Alarm
GPS
System Time
Local System Clocks
Set System Mode
Modem Configuration
Modem Dial Out
Modem Calibrate
Modem Test
Update
Reboot
Holdover
Log Configuration
Daily: Every 0 Days
At 0 :00 UTC Click here to edit or create local system clocks.
Weekly: Every 0 weeks
On: MON TUE WED
THU FRI SAT SUN
At 0 :00 UTC Click here to edit or create local system clocks.
Monthly: Day 0 of every 0 month(s)
First MON of every 0 month(s)
At 0 :00 UTC Click here to edit or create local system clocks.
Yearly: Every: JAN 0
At 0 :00 UTC Click here to edit or create local system clocks.
Boot:
Dialout at boot if not synced after: 0 Days 1 Hours 0 Minutes
Submit
Reset
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Done
Internet

Figure 7-9: System Modem Dial Out Screen (2 of 2)

If the modem is the primary mode of operation for time synchronization, the boot dial-out value should be set for a very short duration as the unit will not be able to achieve time synchronization without the modem placing a call. If the modem is strictly a backup to the external reference, this period can be lengthened to longer than the typical amount of time needed to synchronize to the external reference.

The System Modem Calibrate screen (Figure 7-10) is used to calibrate the modem for increased accuracy of the dial-out calls. The calibration procedure is not required but may be used to provide greater accuracy of future modem calls. The calibration process, using several dial-out helps compensate for inherit internal software processing lags as well as phone network delays as well. Different locations may experience different latencies as well as time of day latencies may also vary.

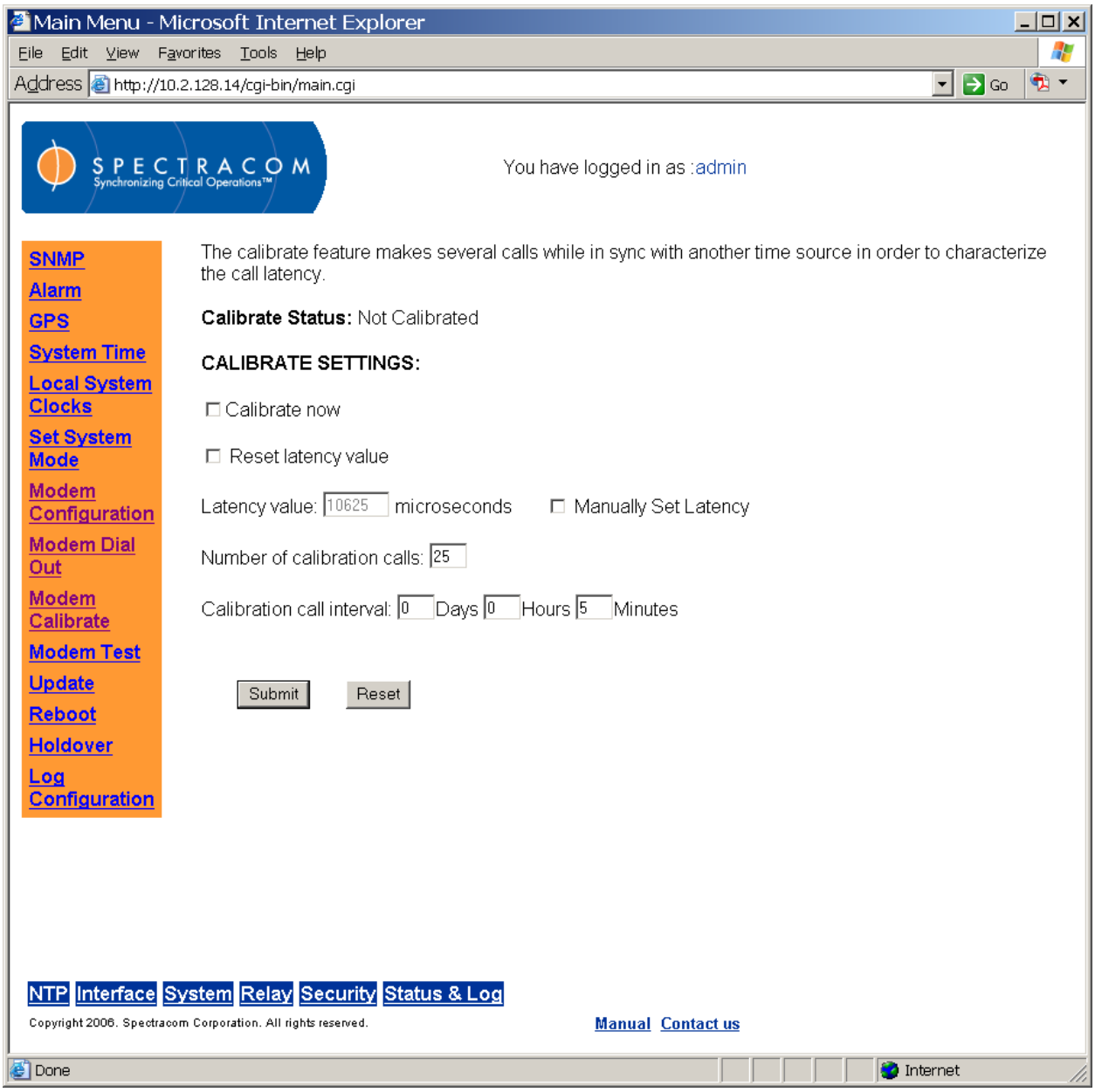


Figure 7-10: System Modem Calibrate Screen

The calibrate mode allows the user to define the typical latency for the geographic location as well as the time of day the modem is most likely to be used for time synchronization (such as for primary mode of operation).

Calibrate Status:
The status of calibration is displayed at the top of the screen. If the calibration has been made then the unit will say “calibrated”. If the latency has not been set or has been manually set, then the unit will say “not calibrated”. If the unit is currently calibrating then the number of successful calls will be displayed here.

Calibrate Settings
Calibrate Now:
Calibrate now is based on the current settings. This will calculate the call latency and adjust all future calls based on this value. The call latency is based primarily on the phone system. Therefore, this should be done when the unit is first set up and does not need to be done again unless it is connected to a different phone system.

Reset Latency Value:
This resets the latency value to the factory default. This can be done if the unit was accidentally set.

Latency Value/Manually Set Latency:
This box displays the current latency value. If the "manually set latency" box is checked then this can be edited to set the current latency.

Number of Calibration calls:
This is the number of calibration calls to be made before the modem is declared as calibrated. The accuracy of the latency calculation depends directly on this number. The more calls that are made, the more accurate the calculation will be. This should not be lowered from the default, but it may be safely raised.

Calibration Call Interval:
This is the interval between calibration calls. This value, along with the number of calibration calls, will determine how long the calibration process will take.

7.1.7 Modem Testing

The modem can be tested using the Web UI through the Modem Test screen (Figure 7-11).

Test Now:
Tests the modem to make sure it can correctly dial-out. This may only be done while in time synchronization from another source such as GPS. To test in other states, use the dial now button. The result of this test will be written to the log file.

Test On Interval:
Enables the modem test interval. If the unit has not made another type of call during this interval then a test call will be made.

Test Interval:
Sets the modem test interval. In order to set these values, the "Test On Interval" box must be checked. If the interval expires before another type of call is made then a modem test call will be made. To schedule a call when not in sync from another time source, use the "Call Interval" setting in the Dialout Settings page.

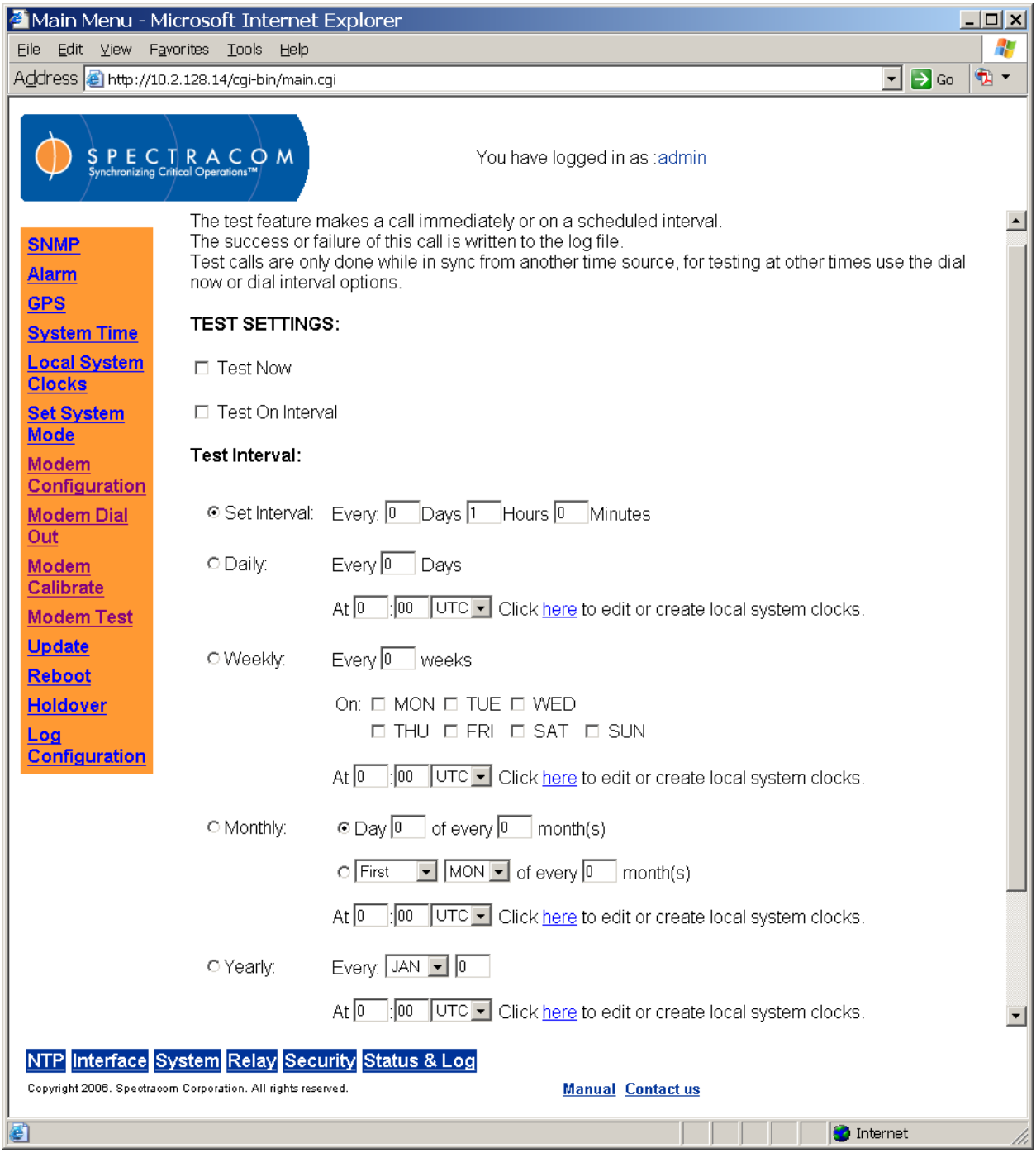

Main Menu - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.2.128.14/cgi-bin/main.cgi
Go
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
SNMP
Alarm
GPS
System Time
Local System Clocks
Set System Mode
Modem Configuration
Modem Dial Out
Modem Calibrate
Modem Test
Update
Reboot
Holdover
Log Configuration
The test feature makes a call immediately or on a scheduled interval.
The success or failure of this call is written to the log file.
Test calls are only done while in sync from another time source, for testing at other times use the dial now or dial interval options.
TEST SETTINGS:
Test Now
Test On Interval
Test Interval:
Set Interval: Every: 0 Days 1 Hours 0 Minutes
Daily: Every 0 Days
At 0 :00 UTC Click here to edit or create local system clocks.
Weekly: Every 0 weeks
On: MON TUE WED THU FRI SAT SUN
At 0 :00 UTC Click here to edit or create local system clocks.
Monthly: Day 0 of every 0 month(s)
First MON of every 0 month(s)
At 0 :00 UTC Click here to edit or create local system clocks.
Yearly: Every: JAN 0
At 0 :00 UTC Click here to edit or create local system clocks.
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Manual Contact us
Internet

Figure 7-11: Modem Test Screen

There are four different types of modem dial-out calls that can be made. The call type is determined by the state of the system (after the call is finished) as well as user input. Calibration calls happen upon a user request. Time verification calls happen on a user specified interval if holdover is entered from time synchronization with another source. Time synchronization calls occur when time synchronization is lost and on a user specified interval until another time source is available. Modem test calls happen when no calls have been made for a user specified time, or upon a user request. Because the modem determines how to use a call after

the call is finished it is possible to start a call as a certain call type and actually use it as another call type. Here is a description of each of the four possible call types.

7.1.7.1 Calibration Call

Calibration calls are done to characterize the call latency. A user specified number of calls will be made over the calibration period and the average latency will be used to adjust all future calls.

NOTE: The calibration will only be done at the user's request and may be started only while in sync from a stratum 0 time source. Calibration calls may be continued into holdover, but will be cut off if the unit goes out of sync at any point during the calibration period.

7.1.7.2 Time Verification Call

Time verification calls are made to verify the unit still has acceptable time and to correct for any leap seconds that may be asserted while the reference is not available. Calls will be made on a user specified time table. If the call interval is more than a month leap seconds may be missed. If a leap second is to be inserted at the end of the month then the clock will be scheduled to do so. If the time is off by more than half a second then the unit will be immediately put into unsynchronized mode (time synchronization lamp will extinguish and time outputs will be ignored).

7.1.7.3 Time Sync Call

Time synchronization calls occur to set the second and sub second timers and to check for any leap seconds. If a call is successful the timer will be set and the unit will be put in holdover mode with the holdover timer reset. In addition if a leap second is to be inserted at the end of the month then the clock will be scheduled to do so. Time synchronization calls will be made once the unit has gone into unsynchronized mode until it obtains sync from another time source. During this period, calls will be made on a user specified timetable or any time the unit goes out of sync.

7.1.7.4 Modem Test Call

Test calls are calls that make sure the modem is working. The modem will call out and check for valid time messages. The unit will log "test passed" if it was able to get good time messages or failed if it was not. No changes will be made to the system time. Testing can be done only in sync from another time source and can either be on a specified interval or as requested.

7.1.8 Verify Modem Operation

For the modem to function with the NetClock, the client mode must be selected in the System Modem Configuration screen for the NetClock to accept the change from console mode.

If the unit is already powered-up and not synchronized, choosing dial-out now and hitting submit will cause the unit to connect to NIST. If the unit is already synchronized, this option is not available (The dialout now function is not available for operation if the NetClock is in either holdover or sync mode). To operate the modem if it is in currently in sync, disconnect the antenna and wait until the variable holdover period expires or power cycle the unit to clear the sync condition. Then, the dial-out now function will be available.

Once the NetClock has dialed and synchronized to NIST, the unit will be in holdover mode until the variable holdover period expires (Devices syncing to the NetClock will still sync) indicated by the sync light flashing green. After the variable holdover expires, the unit will declare loss of sync (Sync lamp turns red) or when the scheduled Time Verification call occurs, the modem automatically dials NIST again. If connection is made, holdover is restored (Sync lamp flashes green again).

Verify proper operation of the modem by observing the status of the front panel sync lamp flashing green after connection to NIST and verifying the Model dial-out logs. The Modem Dialout Log (Figure 7-12) is a running list of the NetClock's modem activity. This log will have no activity if the NetClock is not equipped with a modem or if the modem has not yet been used.

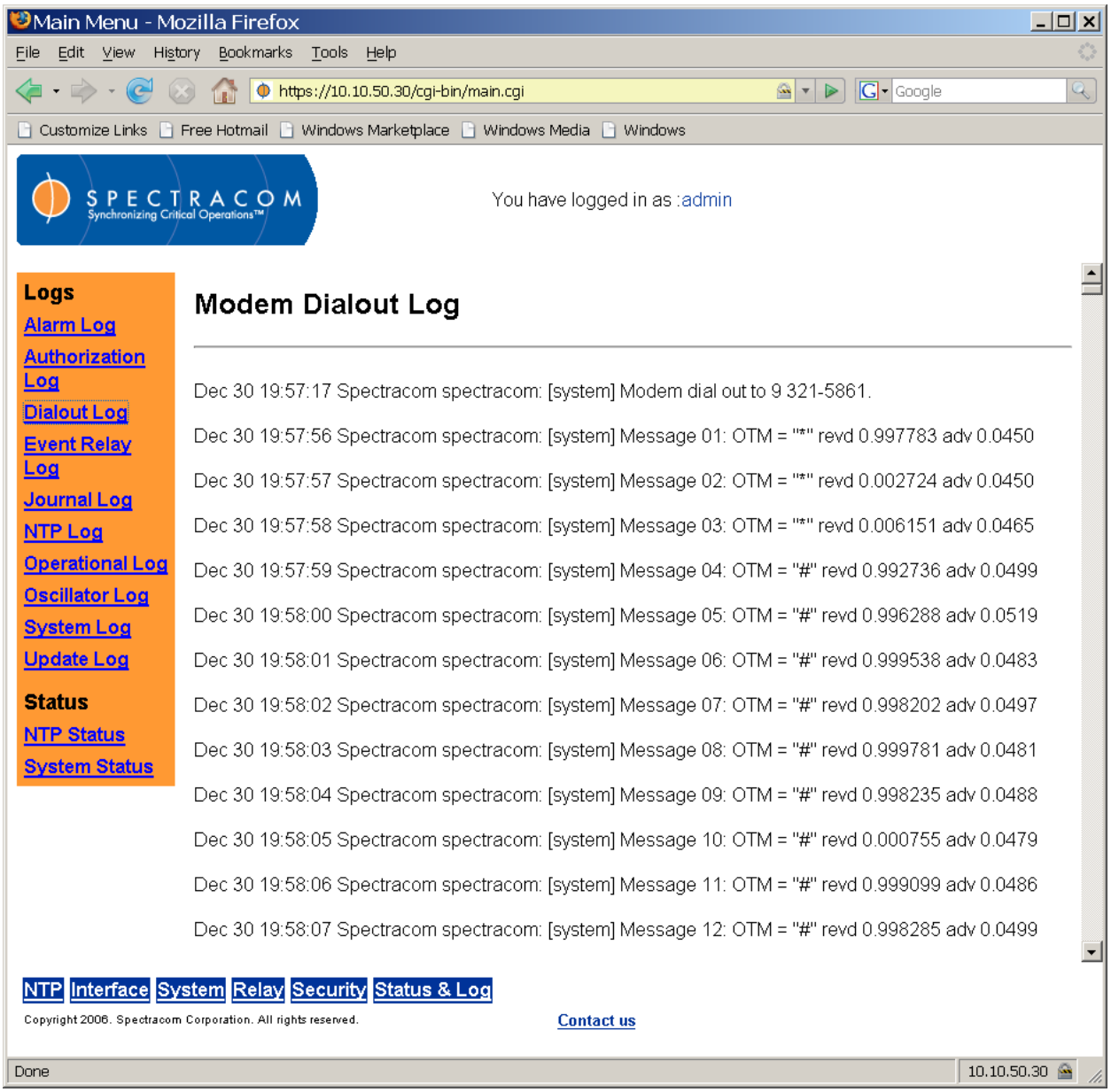

Main Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.10.50.30/cgi-bin/main.cgi
Customize Links Free Hotmail Windows Marketplace Windows Media Windows
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Logs
Alarm Log
Authorization Log
Dialout Log
Event Relay Log
Journal Log
NTP Log
Operational Log
Oscillator Log
System Log
Update Log
Status
NTP Status
System Status
Modem Dialout Log
Dec 30 19:57:17 Spectracom spectracom: [system] Modem dial out to 9 321-5861.
Dec 30 19:57:56 Spectracom spectracom: [system] Message 01: OTM = "*" revd 0.997783 adv 0.0450
Dec 30 19:57:57 Spectracom spectracom: [system] Message 02: OTM = "*" revd 0.002724 adv 0.0450
Dec 30 19:57:58 Spectracom spectracom: [system] Message 03: OTM = "*" revd 0.006151 adv 0.0465
Dec 30 19:57:59 Spectracom spectracom: [system] Message 04: OTM = "#" revd 0.992736 adv 0.0499
Dec 30 19:58:00 Spectracom spectracom: [system] Message 05: OTM = "#" revd 0.996288 adv 0.0519
Dec 30 19:58:01 Spectracom spectracom: [system] Message 06: OTM = "#" revd 0.999538 adv 0.0483
Dec 30 19:58:02 Spectracom spectracom: [system] Message 07: OTM = "#" revd 0.998202 adv 0.0497
Dec 30 19:58:03 Spectracom spectracom: [system] Message 08: OTM = "#" revd 0.999781 adv 0.0481
Dec 30 19:58:04 Spectracom spectracom: [system] Message 09: OTM = "#" revd 0.998235 adv 0.0488
Dec 30 19:58:05 Spectracom spectracom: [system] Message 10: OTM = "#" revd 0.000755 adv 0.0479
Dec 30 19:58:06 Spectracom spectracom: [system] Message 11: OTM = "#" revd 0.999099 adv 0.0486
Dec 30 19:58:07 Spectracom spectracom: [system] Message 12: OTM = "#" revd 0.998285 adv 0.0499
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Done
10.10.50.30

Figure 7-12: Modem Dialout Log Screen

The Modem Dialout Log provides information concerning the numbers dialed, whether the dialouts were successful, and what changes have been applied to the subsecond counter and system clock. If calling a Spectracom ACTS server, additional information about each time message is logged, including the on-time character (what it is, when it is received) and the advance time included in the message.

If the sync lamp is also flashing red, this is because the GPS antenna is disconnected from the NetClock. This is not directly related to the modem dial-out feature but if the antenna has been connected in the past, it is related to the reason why the modem is now dialing-out unexpectedly (Antenna problem causing loss of GPS time Sync).

7.2 Option 04: Rubidium Oscillator

Option 04 provides the NetClock with a self-calibrating ovenized rubidium oscillator. The purpose of this oscillator is to provide a very accurate time base when GPS is either lost or cannot be obtained due to site limitations. It is also used to provide a very stabile and accurate 10 MHz output with a high degree of holdover if GPS is lost. Because of its high degree of stability, this oscillator provides the ability to greatly extend the hold-over period when GPS is not present. Extending the hold-over period allows the unit to provide very accurate and useable time stamps and a 10 MHz output for a longer period of time once time synchronization has been lost.

NOTE: The NetClock must be ordered with Option 04 installed at the time of the initial purchase. This option cannot be added after the NetClock has been shipped from the factory.

The Rubidium oscillator is atomic in nature but requires no MSDS.

7.2.1 Comparison of the Rubidium oscillator to the OCXO and standard TCXO oscillators:

10 MHZ frequency output:

Rubidium oscillator (Option 04): $1x10^{-12}$ typical 24-hour average locked to GPS, $1x10^{-11}$ per month typical aging unlocked.

OCXO oscillator (Option 05): $1x10^{-11}$ typical 24-hour average locked to GPS, $2x10^{-9}$ per week typical aging unlocked.

TCXO oscillator (Standard): $1x10^{-10}$ typical 24-hour average locked to GPS

Time drift while the NetClock is in Holdover mode (Loss of primary/backup reference):

Oscillator	Option	Estimated Error Rates	Time to reach 2 ms
Rb	Option 04	0.18 microseconds / hour (nominal)	463 days
OCXO	Option 05	72 microseconds / hour (nominal)	28 hours
TCXO	Standard	1.0 milliseconds / hour (nominal)	2 hours (typical)
TCXO	Standard	7.2 milliseconds / hour (worst case)	17 minutes*

7.3 Option 05: OCXO Oscillator

Option 05 provides the NetClock with a self-calibrating ovenized quartz oscillator. The purpose of this oscillator is to provide a very accurate time base when GPS is either lost or cannot be obtained due to site limitations and a very precise 10 MHz output. Because of its high degree of stability, this oscillator provides the ability to greatly extend the hold-over period when GPS is not present. Extending the hold-over period allows the unit to provide very accurate and useable time stamps and a 10 MHz output for a longer period of time once time synchronization has been lost.

The OCXO characteristics are not quite the same as the Option 04 Rubidium oscillator, but are still much greater than the standard TCXO that is used in the product when option 4 and 5 are not installed.

NOTE: The NetClock must be ordered with Option 05 installed at the time of the initial purchase. This option cannot be added after the NetClock has been shipped from the factory

7.3.1 Comparison of the OCXO to the Rubidium and Standard TCXO oscillators:

10 MHZ frequency output:

OCXO oscillator (Option 05): $1x10^{-11}$ typical 24-hour average locked to GPS, $2x10^{-9}$ per week typical aging unlocked.

Rubidium oscillator (Option 04): $1x10^{-12}$ typical 24-hour average locked to GPS, $1x10^{-11}$ per month typical aging unlocked.

TCXO oscillator (Standard): $1x10^{-10}$ typical 24-hour average locked to GPS.

Time Drift while the NetClock is in Holdover mode (Loss of primary/backup reference):

Oscillator	Option	Estimated Error Rates	Time to reach 2 ms
OCXO	**Option 05**	**72 microseconds / hour (nominal)**	**28 hours**
Rubidium	Option 04	0.18 microseconds / hour (nominal)	463 days
TCXO	Standard	1.0 milliseconds / hour (nominal)	2 hours (typical)
TCXO	Standard	7.2 milliseconds / hour (worst case)	17 minutes*

7.4 Option 06: IRIG Input

Spectracom NetClock units equipped with Option 06 support IRIG input.

7.4.1 IRIG Input Specifications

Signal: IRIG B, amplitude modulated sine wave (AM) or pulse-width-coded (DCLS, Differential).

AM Carrier: IRIG B 1000 Hz.

AM Signal Level: 500mV to 10V p-p (Modulated 2:1 to 6:1).

DCLS Signal Level: >10k ohms. RS-485 or TTL with DCLS IRIG IN connected to ground.

Connector: AM: BNC female
DCLS RS-485: DB9 female.

IRIG Code Format Provided	Code Description
B000	IRIG B, TTL, BCD,CF and SBS
B120	IRIG B, AM, 1 kHz , BCD,CF and SBS

BNC Connector Pin-out	
Center Pin	IRIG HI
Shield	IRIG LO
DB9 Connector Pin-out	
Pin 1	NC
Pin 2	Ground
Pin 3	Ground
Pin 4	DCLS IRIG IN + (for single ended)
Pin 5	DCLS IRIG IN -
Pin 6	NC
Pin 7	NC
Pin 8	NC
Pin 9	NC

7.4.2 IRIG Input Setup

From the IRIG Input setup screen (Figure 7-13), the user may configure the source year to be used with the IRIG input time code. By default, the year fields in the IRIG message are ignored and a user-defined value is used.

NOTE: Make sure the year is set correctly when the NetClock is installed. If the year is not set correctly before NTP achieves time synchronization, it will use the value entered. The unit will also default to the year entered if it is powered down during the rollover of the year. If the NetClock was not switched on during the rollover, this value must be updated.

NOTE: When the IRIG Input year is updated, the NTP server must be restarted from the NTP Web UI page (or the NetClock rebooted) for the new year value to take effect.

Figure 7-13: IRIG Input Screen

7.5 Option 07: SAASM

The 9300 series NetClock is available with a secure GPS receiver, the Selective Availability/Anti-Spoofing Module (SAASM) option, for use in military GPS applications. Units equipped with the SAASM receiver will display data similar to, but formatted differently than, the data provided by non-SAASM NetClock units.

The NetClock's SAASM receiver can operate in multiple modes. Spectracom supports Standard (Continuous) and Stationary (Averaging) modes. In Stationary mode, the GPS receiver cannot be moving. Spectracom software defaults to the Continuous mode, in which the receiver may or may not be moving.

In Stationary (Averaging) mode, the receiver averages the position data received in order to establish a more accurate position fix over time. Using this mode provides higher jamming immunity compared to Time Only mode.

GPS Data provided by the NetClock SAASM receiver includes:

- Number of GPS satellites tracked
- The GPS status of the unit (position hold or otherwise)
- Antenna sense
- Latitude and longitude of the unit
- Antenna height
- Pass or fail for signal quality

A grid of data (an illustrative portion of which is found in Figure 7-14) provided by the SAASM receiver also includes the GPS Channel, satellite vehicle ID (VID), the mode in which each satellite is operating, the signal strength (under a specific threshold, the satellite signal is not usable), and the status for each satellite.

CHANNEL	VID	MODE	STRENGTH	CODE TYPE	FREQ
1	3	5	43	Y-code	L1
2	29	5	39	Y-code	L1
3	26	5	42	Y-code	L1
4	6	5	43	Y-code	L1

Figure 7-14: GPS Signal Status

7.5.1 Satellite Mode

The satellite modes are as follows:

0 Idle (standby)
1 Normal Acquisition (C/A-code search mode)
2 Direct Acquisition (P[Y]-code search mode)
3 Code Lock (interference)
4 Carrier Lock (degraded tracking mode)
5 Carrier Track/Data Collection (good tracking)
6 Sequential Resynchronization
7 Signal reacquisition (recovery mode)

7.5.2 Satellite Status

The satellite status is a two-digit number. The first digit represents the code type and the second digit represents the antenna frequency. These, in turn, correspond to encrypted/unencrypted statuses.

NOTE: A channel that is tracking no satellites will display a status of 00. This means there is no signal.

7.5.2.1 First Digit: Code Type

0	P-code	Precise Ranging code
1	C/A-code	Coarse Acquisition code
2	Y-code	Encrypted Precise Ranging code

7.5.2.2 Second Digit: Antenna Frequency

0	L1	RF Link, GPS primary frequency, 1575.42 MHz
1	L2	RF Link, GPS primary frequency, 1227.6 MHz

7.5.3 Zeroize

The SAASM receiver includes a zeroize feature, found both in the software screens through the Web User Interface (Figure 7-15) and externally as a physical zeroize button on the face of the NetClock. There are two zeroize modes, Zeroize SA/A-S Keys Only and Emergency Zeroize.

- Selecting Zeroize SA/A-S Keys Only or pressing the button on the face of the unit erases the crypto-variable keys loaded in the SAASM receiver.

- Selecting Emergency Zeroize erases all operational data on the SAASM receiver.

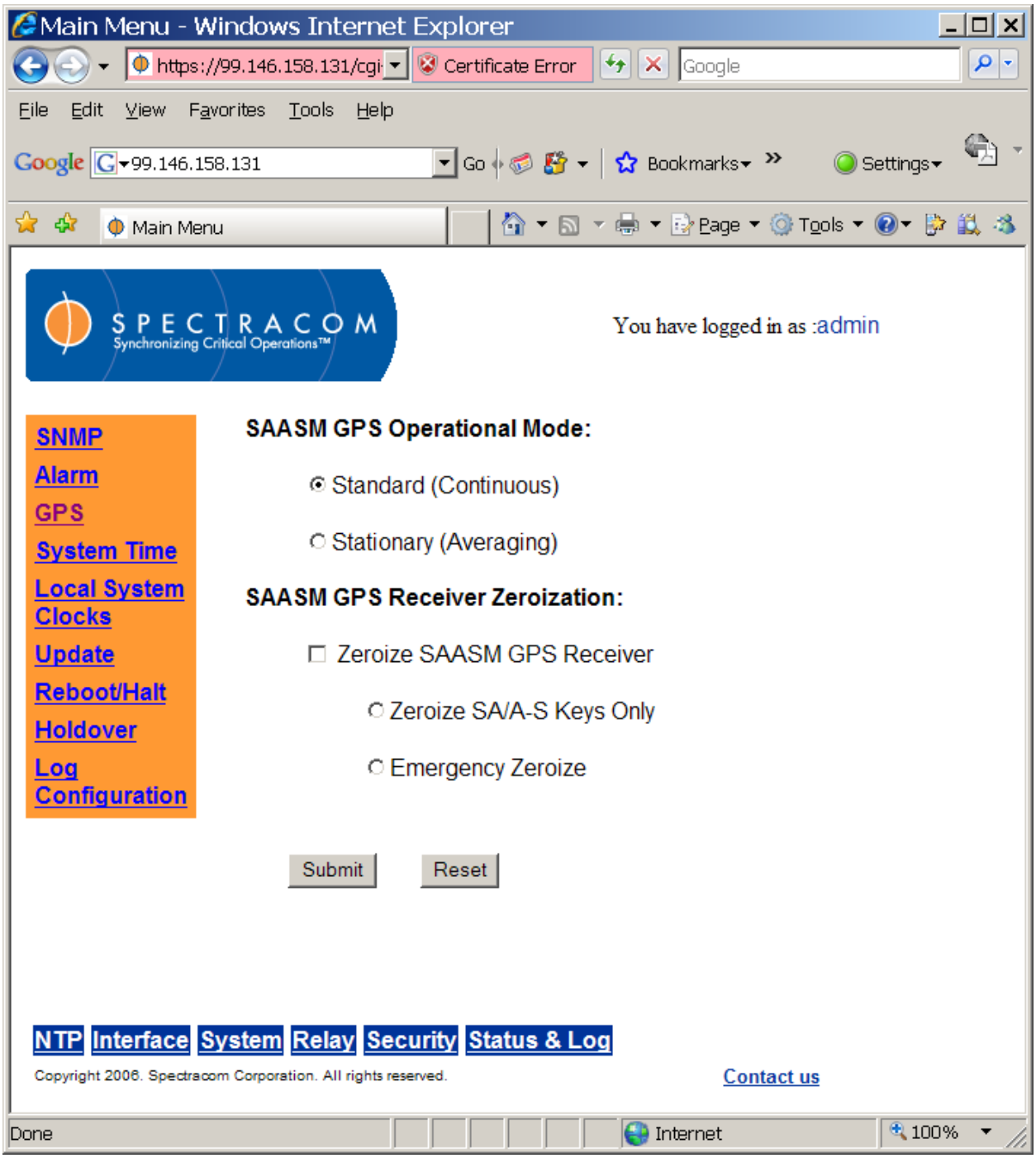


Figure 7-15: Zeroize Screen

7.5.4 Security — SAASM

The SAASM screen, found through the Security menu, lists for the user the software and hardware version information. It also includes the status of the system security keys.

7.6 Option 10: Low Phase Noise Rubidium 10 MHz and Differential IRIG Output

Option 10 provides a low Phase Noise 10 MHz output and a differential IRIG time code output. The standard 9383 NetClock Remote Port 2 is replaced by the Option 10 IRIG Time Code Output. The IRIG output as shipped from the factory is format B-002.

7.6.1 10 MHz Output (FREQ OUT) Specifications

- Sine wave Output
- SSB Phase Noise Specifications in a 1 Hz bandwidth for the 10 MHz Reference Frequency:
    - 1 Hz Offset , - 90 dBc/Hz
    - 10 Hz Offset , -120 dBc/Hz
    - 100 Hz Offset , -135 dBc/Hz
- The 10 MHz output power shall be 10 dBm (± 1 dB) sine-wave into 50 Ω.
- ≤ 1 x 10^{-11} per month in absence of disciplining, or GPS signals when GPS locked
- ≤ 1 x 10^{-12} (for periods up to 100 sec)

7.6.2 IRIG-B Output (Remote Port 2) Specifications

- Differential Output
- B002 Format
- Differential output conforms to RS-485 standard.
- 3 pin Pluggable Terminal Block Connector, pin 1, pin 2, pin 3
- UTC Time

7.6.3 DC Input Power

The DC Input Power is +24 VDC @ 2.5 amps, ± 1%

7.6.4 Rear Panel Connectors

The IRIG-B DIFF OUT is provided on the rear of the NetClock. It replaces the RS-485 REMOTE PORT 2 on the rear panel of the standard NetClock (right).

7.7 Option 11: Modified IRIG Output

Option 11 provides two IRIG outputs and a Format 09 ASCII serial time code. These outputs and the Format 09 time code are fixed. The IRIG OUT and 1PPS IN ports on the rear of the standard 9383 NetClock are replaced by the Option 11 IRIG-B and IRIG-E outputs specified herein. The standard 9383 NetClock's SERIAL COMM 2 port is replaced by the Option 11 ASCII Time Code Output port.

NOTE: The Option 11 outputs will NOT function until the unit has synchronized to GPS. Thereafter, the outputs will continue to function even if the NetClock is in Holdover mode.

7.7.1 IRIG-B Output Specifications

- AM Output
- B126 Format
- Fixed amplitude of 5 Vpp into no load
- BNC Connector
- UTC Time

7.7.2 IRIG-E Output Specifications

- AM Output
- E126 Format
- Fixed amplitude of 5 Vpp into no load
- BNC Connector
- UTC Time

7.7.3 ASCII Time Code Output (Format 09)

- RS-232, DB-9 Connector
- UTC Time
- 9600 baud, 1 start bit, 7 data bits, 1 stop bit and even parity in the format **<SOH>DDD:HH:MM:SSQ<CR><LF>** where:

  <SOH> = Start of header (ASCII Character 1)
  DDD = Day of Year (001-366)
  : = Colon Separator
  HH = Hours (00-23)
  MM = Minutes (00-59)
  SS = Seconds (00-59), (00-60 for leap second)
  Q = Time Sync Status (space = SYNC, "?" = NOT SYNC)
  <CR> = Carriage Return (ASCII Character 13)
  <LF> = Line Feed (ASCII Character 10)

NOTE: The carriage return character <CR> start bit begins on the second (on time point).

7.7.4 DC Input Power

The DC Input Power is +12 VDC @ 2.5 amps, ± 1%

7.7.5 Serial Port 2 (Format 09) Configuration

The NetClock's SERIAL FMT09 port ships from the factory properly configured for Format 09. If changes occur in the field that require reconfiguration of the ASCII Serial Time Code output for Format 09, the user may make these changes from the NetClock's Interface menu. This is found within the Web User Interface and groups the NetClock's Interface configuration functions. From this menu, the user may access the Interface Serial Port, Remote Port, IRIG, Display, and Frequency Output screens for the standard 9383 NetClock. For Option 11, Serial Port 2 must be configured as follows. (The unit reads Serial Port 2 as SERIAL FMT09 when Option 11 is installed. This change does not affect Serial Port 1, which operates according to standard 9383 specifications).

Main Menu - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.10.128.59/cgi-bin/main.cgi
My Stuff INFO STUFF Work Info Tech Info Computer Stuff Venders RoHS Info Shopping NTP INFO TNC/N
SPECTRACOM
Synchronizing Critical Operations™
You have logged in as :admin
Serial Port 1
Serial Port 2
Remote Port 1
Remote Port 2
Front Panel Display
Frequency Output
Set To Defaults
BAUD RATE: 9600
DATA FORMAT: 02
REQUEST CHAR: Multicast User defined T
SYSTEM CLOCK: UTC Click here to edit or create local system clocks.
Submit Reset
NTP Interface System Relay Security Status & Log
Copyright 2006. Spectracom Corporation. All rights reserved.
Contact us
Done
10.10.128.59

Figure 7-16: Serial Port Configuration

- The baud rate must be set to 9600.
- The data format must be set to 02.
- The request char must be set to Multicast.
- The system clock must be set to UTC.

7.7.6 Rear Panel Connectors

The IRIG-B OUT, IRIG-E Out, and SERIAL FMT09 ports are labeled on the rear of the NetClock. They replace the IRIG OUT, 1PPS IN, and SERIAL COMM 2 ports on the rear panel of the NetClock.

8 License Notices

This file is automatically generated from html/copyright.htm

Copyright Notice

[sheepb.jpg] "Clone me," says Dolly sheepishly

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

```
*********************************************************************
*                                   *
* Copyright (c) David L. Mills 1992-2001              *
*                                   *
* Permission to use, copy, modify, and distribute this software and  *
* its documentation for any purpose and without fee is hereby     *
* granted, provided that the above copyright notice appears in all  *
* copies and that both the copyright notice and this permission    *
* notice appear in supporting documentation, and that the name    *
* University of Delaware not be used in advertising or publicity   *
* pertaining to distribution of the software without specific,    *
* written prior permission. The University of Delaware makes no    *
* representations about the suitability this software for any     *
* purpose. It is provided "as is" without express or implied     *
* warranty.                           *
*                                   *
*********************************************************************
```

The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

1. [1]Mark Andrews <marka@syd.dms.csiro.au> Leitch atomic clock controller
2. [2]Bernd Altmeier <altmeier@atlsoft.de> hopf Elektronik serial line and PCI-bus devices
3. [3]Viraj Bais <vbais@mailman1.intel.com> and [4]Clayton Kirkwood <kirkwood@striderfm.intel.com> port to WindowsNT 3.5
4. [5]Michael Barone <michael,barone@lmco.com> GPSVME fixes
5. [6]Karl Berry <karl@owl.HQ.ileaf.com> syslog to file option
6. [7]Greg Brackley <greg.brackley@bigfoot.com> Major rework of WINNT port. Clean up recvbuf and iosignal code into separate modules.
7. [8]Marc Brett <Marc.Brett@westgeo.com> Magnavox GPS clock driver
8. [9]Piete Brooks <Piete.Brooks@cl.cam.ac.uk> MSF clock driver, Trimble PARSE support
9. [10]Reg Clemens <reg@dwf.com> Oncore driver (Current maintainer)
10. [11]Steve Clift <clift@ml.csiro.au> OMEGA clock driver
11. [12]Casey Crellin <casey@csc.co.za> vxWorks (Tornado) port and help with target configuration
12. [13]Sven Dietrich <sven_dietrich@trimble.com> Palisade reference clock driver, NT adj. residuals, integrated Greg's Winnt port.
13. [14]John A. Dundas III <dundas@salt.jpl.nasa.gov> Apple A/UX port
14. [15]Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de> Linux port
15. [16]Dennis Ferguson <dennis@mrbill.canet.ca> foundation code for NTP Version 2 as specified in RFC-1119
16. [17]Glenn Hollinger <glenn@herald.usask.ca> GOES clock driver
17. [18]Mike Iglesias <iglesias@uci.edu> DEC Alpha port
18. [19]Jim Jagielski <jim@jagubox.gsfc.nasa.gov> A/UX port
19. [20]Jeff Johnson <jbj@chatham.usdesign.com> massive prototyping overhaul
20. [21]Hans Lambermont <Hans.Lambermont@nl.origin-it.com> or [22]<H.Lambermont@chello.nl> ntpsweep
21. [23]Poul-Henning Kamp <phk@FreeBSD.ORG> Oncore driver (Original author)
22. [24]Frank Kardel [25]<Frank.Kardel@informatik.uni-erlangen.de> PARSE <GENERIC> driver (14 reference clocks), STREAMS modules for PARSE, support scripts, syslog cleanup
23. [26]William L. Jones <jones@hermes.chpc.utexas.edu> RS/6000 AIX modifications, HPUX modifications
24. [27]Dave Katz <dkatz@cisco.com> RS/6000 AIX port
25. [28]Craig Leres <leres@ee.lbl.gov> 4.4BSD port, ppsclock, Magnavox GPS clock driver
26. [29]George Lindholm <lindholm@ucs.ubc.ca> SunOS 5.1 port
27. [30]Louis A. Mamakos <louie@ni.umd.edu> MD5-based authentication
28. [31]Lars H. Mathiesen <thorinn@diku.dk> adaptation of foundation code for Version 3 as specified in RFC-1305
29. [32]David L. Mills <mills@udel.edu> Version 4 foundation: clock discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG
30. [33]Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de> VMS port
31. [34]Jeffrey Mogul <mogul@pa.dec.com> ntptrace utility
32. [35]Tom Moore <tmoore@fievel.daytonoh.ncr.com> i386 svr4 port
33. [36]Kamal A Mostafa <kamal@whence.com> SCO OpenServer port
34. [37]Derek Mulcahy <derek@toybox.demon.co.uk> and [38]Damon Hart-Davis <d@hd.org> ARCRON MSF clock driver
35. [39]Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de> monitoring/trap scripts, statistics file handling
36. [40]Dirce Richards <dirce@zk3.dec.com> Digital UNIX V4.0 port
37. [41]Wilfredo Sánchez <wsanchez@apple.com> added support for NetInfo
38. [42]Nick Sayer <mrapple@quack.kfu.com> SunOS streams modules
39. [43]Jack Sasportas <jack@innovativeinternet.com> Saved a Lot of space on the stuff in the html/pic/ subdirectory
40. [44]Ray Schnitzler <schnitz@unipress.com> Unixware1 port
41. [45]Michael Shields <shields@tembel.org> USNO clock driver
42. [46]Jeff Steinman <jss@pebbles.jpl.nasa.gov> Datum PTS clock driver
43. [47]Harlan Stenn <harlan@pfcs.com> GNU automake/autoconfigure makeover, various other bits (see the ChangeLog)
44. [48]Kenneth Stone <ken@sdd.hp.com> HP-UX port
45. [49]Ajit Thyagarajan <ajit@ee.udel.edu>IP multicast/anycast support
46. [50]Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp>TRAK clock driver
47. [51]Paul A Vixie <vixie@vix.com> TrueTime GPS driver, generic TrueTime clock driver
48. [52]Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de> corrected and validated HTML documents according to the HTML DTD

---

[53]gif

[54]David L. Mills <mills@udel.edu>

References

1. mailto:marka@syd.dms.csiro.au
2. mailto:altmeier@atlsoft.de
3. mailto:vbais@mailman1.intel.co
4. mailto:kirkwood@striderfm.intel.com
5. mailto:michael.barone@lmco.com
6. mailto:karl@owl.HQ.ileaf.com
7. mailto:greg.brackley@bigfoot.com
8. mailto:Marc.Brett@westgeo.com
9. mailto:Piete.Brooks@cl.cam.ac.uk
10. mailto:reg@dwf.com
11. mailto:clift@ml.csiro.au
12. mailto:casey@csc.co.za
13. mailto:Sven_Dietrich@trimble.COM
14. mailto:dundas@salt.jpl.nasa.gov
15. mailto:duwe@immd4.informatik.uni-erlangen.de
16. mailto:dennis@mrbill.canet.ca
17. mailto:glenn@herald.usask.ca
18. mailto:iglesias@uci.edu
19. mailto:jagubox.gsfc.nasa.gov
20. mailto:jbj@chatham.usdesign.com
21. mailto:Hans.Lambermont@nl.origin-it.com
22. mailto:H.Lambermont@chello.nl
23. mailto:phk@FreeBSD.ORG
24. http://www4.informatik.uni-erlangen.de/~kardel
25. mailto:Frank.Kardel@informatik.uni-erlangen.de
26. mailto:jones@hermes.chpc.utexas.edu
27. mailto:dkatz@cisco.com
28. mailto:leres@ee.lbl.gov
29. mailto:lindholm@ucs.ubc.ca
30. mailto:louie@ni.umd.edu
31. mailto:thorinn@diku.dk
32. mailto:mills@udel.edu
33. mailto:moeller@gwdgv1.dnet.gwdg.de
34. mailto:mogul@pa.dec.com
35. mailto:tmoore@fievel.daytonoh.ncr.com
36. mailto:kamal@whence.com
37. mailto:derek@toybox.demon.co.uk
38. mailto:d@hd.org
39. mailto:Rainer.Pruy@informatik.uni-erlangen.de
40. mailto:dirce@zk3.dec.com
41. mailto:wsanchez@apple.com
42. mailto:mrapple@quack.kfu.com
43. mailto:jack@innovativeinternet.com
44. mailto:schnitz@unipress.com
45. mailto:shields@tembel.org
46. mailto:pebbles.jpl.nasa.gov
47. mailto:harlan@pfcs.com
48. mailto:ken@sdd.hp.com
49. mailto:ajit@ee.udel.edu
50. mailto:tsuruoka@nc.fukuoka-u.ac.jp
51. mailto:vixie@vix.com
52. mailto:Ulrich.Windl@rz.uni-regensburg.de
53. file://localhost/backroom/ntp-stable/html/index.htm
54. mailto:mills@udel.edu

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

```
1)
   * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
   *          All rights reserved
   *
   * As far as I am concerned, the code I have written for this
software
   * can be used freely for any purpose. Any derived versions of this
   * software must be clearly marked as such, and if the derived work
is
   * incompatible with the protocol description in the RFC file, it
must be
   * called by a name other than "ssh" or "Secure Shell".

  [Tatu continues]
   * However, I am not implying to give any licenses to any patents or
   * copyrights held by third parties, and the software includes parts
that
   * are not under my direct control. As far as I know, all included
   * source code is used in accordance with the relevant license
agreements
   * and can be used freely for any purpose (the GNU license being the
most
   * restrictive); see below for details.
```

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library

```
   - RC4 support has been replaced with ARC4 support from OpenSSL
   - Blowfish is now external, in the OpenSSL library

  [The licence continues]

  Note that any information and cryptographic algorithms used in this
  software are publicly available on the Internet and at any major
  bookstore, scientific library, and patent office worldwide. More
  information can be found e.g. at "http://www.cs.hut.fi/crypto".

  The legal status of this program is some combination of all these
  permissions and restrictions. Use only at your own responsibility.
  You will be responsible for any legal consequences yourself; I am not
  making any claims whether possessing or using this is legal or not in
  your country, and I am not taking any responsibility on your behalf.

                                NO WARRANTY

  BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY
  FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT
WHEN
  OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER
PARTIES
  PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER
EXPRESSED
  OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
  MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK
AS
  TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE
  PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY
SERVICING,
  REPAIR OR CORRECTION.

  IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
  WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
  REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR
DAMAGES,
  INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES
ARISING
  OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT
LIMITED
  TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED
BY
  YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY
OTHER
  PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
  POSSIBILITY OF SUCH DAMAGES.

2)
  The 32-bit CRC implementation in crc32.c is due to Gary S. Brown.
  Comments in the file indicate it may be used for any purpose without
  restrictions:

   * COPYRIGHT (C) 1986 Gary S. Brown. You may use this program, or
   * code or tables extracted from it, as desired without restriction.

3)
  The 32-bit CRC compensation attack detector in deattack.c was
  contributed by CORE SDI S.A. under a BSD-style license.

   * Cryptographic attack detector for ssh - source code
   *
   * Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.
   *
   * All rights reserved. Redistribution and use in source and binary
   * forms, with or without modification, are permitted provided that
   * this copyright notice is retained.
   *
   * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED
   * WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE
   * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR
   * CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS
   * SOFTWARE.
   *
   * Ariel Futoransky <futo@core-sdi.com>
   * <http://www.core-sdi.com>

4)
  ssh-keygen was contributed by David Mazieres under a BSD-style
  license.

   * Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
   *
   * Modification and redistribution in source and binary forms is
   * permitted provided that due credit is given to the author and the
   * OpenBSD project by leaving this copyright notice intact.

5)
  The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers
  and Paulo Barreto is in the public domain and distributed
  with the following license:

   * @version 3.0 (December 2000)
   *
   * Optimised ANSI C code for the Rijndael cipher (now AES)
   *
   * @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
   * @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
   * @author Paulo Barreto <paulo.barreto@terra.com.br>
   *
   * This code is hereby placed in the public domain.
   *
   * THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY EXPRESS
   * OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
   * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
   * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE
   * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY,
OR
   * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
OF
   * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
   * BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,
   * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE
   * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
   * EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6)
  One component of the ssh source code is under a 4-clause BSD license,
  held by the University of California, since we pulled these parts
from
  original Berkeley code. The Regents of the University of California
  have declared that term 3 is no longer enforceable on their source
code,
  but we retain that license as is.

   * Copyright (c) 1983, 1990, 1992, 1993, 1995
   *   The Regents of the University of California. All rights
reserved.
   *
   * Redistribution and use in source and binary forms, with or without
   * modification, are permitted provided that the following conditions
   * are met:
   * 1. Redistributions of source code must retain the above copyright
   *  notice, this list of conditions and the following disclaimer.
   * 2. Redistributions in binary form must reproduce the above
copyright
   *  notice, this list of conditions and the following disclaimer in
the
   *  documentation and/or other materials provided with the
distribution.
   * 3. All advertising materials mentioning features or use of this
software
   *  must display the following acknowledgement:
   *   This product includes software developed by the University of
   *   California, Berkeley and its contributors.
   * 4. Neither the name of the University nor the names of its
contributors
   *  may be used to endorse or promote products derived from this
software
   *  without specific prior written permission.
   *
   * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS
IS'' AND
   * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE
   * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
   * ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE
LIABLE
   * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
   * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS
   * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
   * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT
   * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY
   * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF
   * SUCH DAMAGE.

7)
  Remaining components of the software are provided under a standard
  2-term BSD licence with the following names as copyright holders:

            Markus Friedl
            Theo de Raadt
            Niels Provos
            Dug Song
            Aaron Campbell
            Damien Miller
            Kevin Steves
            Daniel Kouril
            Per Allansson

   * Redistribution and use in source and binary forms, with or without
   * modification, are permitted provided that the following conditions
   * are met:
   * 1. Redistributions of source code must retain the above copyright
   *  notice, this list of conditions and the following disclaimer.
   * 2. Redistributions in binary form must reproduce the above
copyright
   *  notice, this list of conditions and the following disclaimer in
the
   *  documentation and/or other materials provided with the
distribution.
   *
   * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS
OR
   * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES
   * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED.
   * IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,
   * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT
   * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS
OF USE,
   * DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY
   * THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
TORT
   * (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF
   * THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



 LICENSE ISSUES
 ==============
```

```
 The OpenSSL toolkit stays under a dual license, i.e. both the
conditions of
 the OpenSSL License and the original SSLeay license apply to the
toolkit.
 See below for the actual license texts. Actually both licenses are
BSD-style
 Open Source licenses. In case of any license issues related to OpenSSL
 please contact openssl-core@openssl.org.

 OpenSSL License
 ---------------

/* ====================================================================
 * Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *  notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *  notice, this list of conditions and the following disclaimer in
 *  the documentation and/or other materials provided with the
 *  distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *  software must display the following acknowledgment:
 *  "This product includes software developed by the OpenSSL Project
 *  for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be
used to
 *  endorse or promote products derived from this software without
 *  prior written permission. For written permission, please contact
 *  openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *  nor may "OpenSSL" appear in their names without prior written
 *  permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *  acknowledgment:
 *  "This product includes software developed by the OpenSSL Project
 *  for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com). This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long
as
 * the following conditions are aheared to. The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 * included with this distribution is covered by the same copyright
terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given
attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *  notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *  notice, this list of conditions and the following disclaimer in the
 *  documentation and/or other materials provided with the
distribution.
 * 3. All advertising materials mentioning features or use of this
software
 *  must display the following acknowledgement:
 *  "This product includes cryptographic software written by
 *   Eric Young (eay@cryptsoft.com)"
 *  The word 'cryptographic' can be left out if the rouines from the
library
 *  being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative
thereof) from
 *  the apps directory (application code) you must include an
acknowledgement:
 *  "This product includes software written by Tim Hudson
(tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
 * ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE
LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available
version or
 * derivative of this code cannot be changed. i.e. this code cannot
simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */

---- Part 1: CMU/UCD copyright notice: (BSD like) -----
    Copyright 1989, 1991, 1992 by Carnegie Mellon University
                        Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California
                                    All Rights Reserved
Permission to use, copy, modify and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appears in all copies and
that both that copyright notice and this permission notice appear in
supporting documentation, and that the name of CMU and The Regents of
the University of California not be used in advertising or publicity
pertaining to distribution of the software without specific written
permission.
CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL
WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR
THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF
CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD)
-----
Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:
* Redistributions of source code must retain the above copyright
notice,
  this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
* Neither the name of the Networks Associates Technology, Inc nor the
  names of its contributors may be used to endorse or promote
  products derived from this software without specific prior written
  permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----
Portions of this code are copyright (c) 2001-2003, Cambridge Broadband
Ltd.
All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:
* Redistributions of source code must retain the above copyright
notice,
  this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
* The name of Cambridge Broadband Ltd. may not be used to endorse or
  promote products derived from this software without specific prior
  written permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
```

OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----
Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa
Clara,
California 95054, U.S.A. All rights reserved.
Use is subject to license terms below.
This distribution may include materials developed by third parties.
Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or
registered
trademarks of Sun Microsystems, Inc. in the U.S. and other countries.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:
* Redistributions of source code must retain the above copyright
notice,
  this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
* Neither the name of the Sun Microsystems, Inc. nor the
  names of its contributors may be used to endorse or promote
  products derived from this software without specific prior written
  permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----
Copyright (c) 2003-2004, Sparta, Inc
All rights reserved.
Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:
* Redistributions of source code must retain the above copyright
notice,
  this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.
* Neither the name of the Networks Associates Technology, Inc nor the
  names of its contributors may be used to endorse or promote
  products derived from this software without specific prior written
  permission.
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE

This open software is available for at least three
  years, to give any third party, for a charge no more than your
  cost of physically performing source distribution, a complete
  machine-readable copy of the corresponding source code, to be
  distributed under the terms of Sections 1 and 2 above on a medium
  customarily used for software interchang

REVISION HISTORY

Revision Level	*ECN*	*Description*
A	**2081**	First-generation manual for the 9300 series products (preceded by a demo manual), current to software rev. Subsequent revision to follow. Changes incorporated from Rev 1 to Rev A include addition of IPSec material, FTP Statistics material, and format reconfiguration, as well as various software changes and other minor corrections. “Log clear” command has been removed.
B	**2156**	Revision to bring manual current to 3.4.0 NetClock software. Changes include adding HALT information in System Configuration, revising NTP section, and adding product configuration/options table.
C	**2210**	Updated SAASM section. Changed antenna cable delay range to ± 50,000,000 nanoseconds. Clarified regions for Australia-1 and Australia-2 DST rules. Added note concerning IRIG Input Year and Serial Time Code Year requiring restart on change. Added Serial Time Code Setup section, which applies to 9388 models only. Added note concerning IRIG Input Year and Serial Time Code Year requiring restart on change. Added note regarding restarting modem if passwords change and when switching between Client and Console modes. Changed System GPS Screen (cable delay change). Added IRIG code descriptions.
D	**2270**	Corrected RS-485 port pin-out depiction. Clarified data format matching issue when using 9388 units.
E	**2328**	“Class B Digital Device” changed to “Class A Digital Device” as FCC notification. Modified note in installation summary concerning NTP synchronization. Added a note to the Oscillator log page concerning FREQ ERROR notation. Add the IRIG codes for IRIG Input. Verified specifications stated in Option 06. Added Option 11. Updated HyperTerminal references (screenshots) in initial setup.
E	**2330**	Changed modem section to reflect upgrade to modem cable (adapter included) and change of modem, with DIP switch settings. (The current revision level of the manual remains “E” — changes made concurrently with previous ECN.)
F	**2313**	Added Option 10.
G	**2354**	Added instructions for restoring factory default settings and deleting position data. Clarified requirement for modem test and calibration calls in Modem section (stratum 0 sync required). Added stc CLI commands. Modified HTTPS and NTP configuration sections to reflect changes in firmware version 3.4.3.

Spectracom Corporation
95 Methodist Hill Drive
Rochester, NY 14623
www.spectracomcorp.com
Phone: US +1.585.321.5800
Fax: US +1.585.321.5219